PENTAGON FORCE PROTECTION AGENCY
“Protecting Those Who Protect Our Nation”

PROTECT YOURSELF

A Guide to Best Practices for Keeping You and Yours Safe Online

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

As your protection-providing organization within the Department of Defense, the Pentagon Force Protection Agency (PFPA) has a unique responsibility for safeguarding your security, and we take that responsibility seriously.

In an age when constant connectivity is an essential part of our daily lives, maintaining a vigilant online posture is particularly important to protecting our personally identifiable information. Those who are not careful can become victims of unwanted personal information collection, resulting in the possible fraudulent use of their information, to include identity theft. Much of this information can be collected when we visit websites, use apps and smart devices, or connect with others on social networks.

It is important to understand the vulnerabilities of an online presence and keep abreast of the most current practices to protect ourselves and our families.

The Protect Yourself guide is divided into 11 color-coded chapters. These key topics, tips, and step-by-step guides mitigate unwanted data exposure to better protect you and your loved ones' privacy.

Semper Vigilans,

Daniel P. Walsh
Acting Director, Pentagon Force Protection Agency

Contents

Protect Yourself: Mobile Devices

MOBILE DEVICES SECURITY BEST PRACTICES

Here are a few precautions you can take to help proactively protect your mobile device, whether it be a smart phone, laptop, or tablet, and the data therein:

Secure Device with a Strong Password

Securing your device with a strong password is the simplest way to secure your device from unauthorized users. You may also be able to set up your device to automatically erase all of your data after a certain number of failed password entry attempts. Consider enabling a time-lock to secure your device while not in use. Also, many modern devices tout biometric capabilities to unlock it, which minimizes the risk of "shoulder-surfing," or individuals looking over your shoulder to see your passcode.

- A four-digit passcode is better than nothing, but a longer and more complex alpha-numeric password will decrease the likelihood your device can be cracked. For pattern-lock devices, pick a complex, unique pattern. Use two-factor verification when you can.
- Third party applications (app), such as "Smart Phone Lock," allow you to secure portions of a phone, such as e-mail, documents, and pictures with a secondary passcode or password, in the event a device is lost or stolen while unlocked.

Treat Your Device like a Computer

Always remember that your smartphone or tablet is a computer. The security precautions you take with your device should mirror the precautions you take with your personal computer.

- Keep the Operating System (OS) up to date; install the latest approved security updates
- Use a reputable antivirus/anti-malware app on your smartphone or tablet

Install Apps Cautiously

Beware of potential third-party manufacturers of apps. In 2013, one popular survey suggested 1.6 million users had been fooled into installing what seemed to be a well-known brand-name app but was actually a malicious imposter. According to a U.S. computer security company, the number of mobile malware apps has steadily risen since 2015.

- Users with government-issued mobile devices will use the DISA Mobile App Store. This online digital electronic software distribution system allows users to browse and download approved apps for their Apple or Andriod commercial mobile devices.
- iPhone users have one source for apps: The App Store. If you use an Android-based phone, you can get apps from numerous sources. Stick with the two most reputable, Google Play and Amazon's Appstore. Google Play Protect can automatically scan your Android device for malware when you install programs. You can ensure it is on and scanning by going to Settings > Security > Play Protect. For maximum security, click "Full scanning," and "Scan device for security threats."

  Realize malicious apps do exist on reputable app stores. In November 2018, Google Play discovered thirteen popular apps that were affected with malware.
- You should be wary of apps that you can download onto your iPhone for free; some criminals are able to tamper with popular apps and infect them with viruses or malware.
- If you are an Android user, you can minimize exposing your privacy by refusing to install an app if it asks to use phone features you do not want it to use. A flashlight app, for example, should not ask to access your location, like the "Brightest Flashlight Free" app did.
- Install a "phone finder" app. These apps are designed to help you find your phone if it becomes lost or stolen.
- Remove "permissions" from apps you do not want to have access to your microphone or camera. Do this by opening settings and scrolling down to the list of apps and individually choosing the permissions for each app.

Beware of Personal Information Stored on Apps

As well as limiting permissions used by apps, you should also limit personal information you publish on an app. If a field does not require to be filled out, do not fill it out. Additionally, do not store credit card information on apps.

- Avoid doing business using free public WiFi; check its privacy policy to see whether it secures WiFi transmission of such data. Only use WiFi with VPN. Otherwise, you may disclose an account number or password to a nearby criminal.
- Be extremely cautious if you decide to use your device for online banking or just accessing your bank account. Making online transactions on a public, unsecure Wi-Fi network could seriously compromise your account's security.
- Only send information thru websites that are fully encrypted. (HTTPS)

Do Not Reply or Click On Text Spam

Links in text spam can lead to websites that download malicious software or to fake websites. The safest practice is to avoid clicking on unfamiliar links within a text. Many smartphone carriers have an option for blocking fake numbers, as well as a spam-detection service.

Disable Location Tracking

Disable location tracking except when you need it, such as for driving directions or finding a nearby store. Most mobile phone operating systems lets you selectively disable for individual apps, use that feature for greater control.

- Turn off "Location" services for your apps if you are seeking more privacy. Companies such as Google, while disabling "Location" tracking, will still be able to track your whereabouts through "Location History," which is also stored under "My Activity" under "Web and App Activity." You can see the stored location markers of your Google profile at myactivity.google.com, although they are typically scattered under several different headers, many of which are unrelated to location.

Register Your Home and Cellular Telephones with the National Do Not Call Registry

Federal Trade Commission's https://www.donotcall.gov - The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls. Most telemarketers should not call your number once it has been on the registry for 31 days. You can refister your home or mobile phone for free.

If you do recieve unwanted calls from telemarketers after your number has been on the registry for 31 days, you can report it. Report unwanted calls at https://www.donotcall.gov and choose "Report Unwanted Calls."

CyberHOUND says ...

We'll help you sniff out the bad guys! Stay Safe Online!

Protect Yourself: Wi-Fi & Bluetooth

WI-FI SECURITY

Wi-Fi, while convenient, is one of the most exploitable weaknesses in your technological defense. It is a single point of failure for every device on the network. You should be over protective of your own and highly suspicious of public networks and those owned by other parties. Bluetooth is similarly exploitable and can allow criminals to bypass your other security measures. For both of these connection types, you should always stay up to date and know how to restrict access.

Update Your Personal Wi-Fi Firmware, or Software System

- Obtain your router internet protocol (IP) address and do an internet search to access your router's web dashboard. Store this number in a secure place.
- After entering the router's IP address into a web browser, log in to the base station with your unique router-name and password. In the router's web dashboard, click on the firmware settings. Look for an option that allows you to check for the latest firmware version. If an update is an option, install and let the router restart. Repeat this process as updates become available.
- You should contact your internet service provider's customer services department to make sure their equipment and firmware are up to date.
- If your device has reached the end of its lifecycle where a manufacturer has stopped supporting firmware updates, it is time to replace the router.

DANGERS USING PUBLIC WI-FI NETWORKS

Take precautions when connecting to a public Wi-Fi network. If possible, use a virtual private network (VPN), which allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more. Be aware that simply connecting through a VPN does not ensure complete protection of your system.

- While most web-based e-mail providers now provide HTTPS/SSL encryption, users must ensure to update their versions to the most recent clients. Use of e-mail services without HTTPS/SSL encryption means nefarious actors can capture your login details and view your email messages.
- Instant messaging and FTP file transfers are vulnerable to Wi-Fi hackers. These services transfer their data in easy to read text, including the login credentials. These login credentials and messages may be vulnerable to hackers when accessed via email software, such as Microsoft Outlook, over an unsecured network.
- Hackers can also connect to your laptop or other Wi-Fi device. You are vulnerable if you have configured your system to share any folders. These folders are also shared on public networks, so other hotspot users can access them if they are not password-protected.
- You may also be vulnerable to man-in-the-middle attacks, where a hacker deliberately mimics a legitimate connection to intercept information from your computer. The hacker can then use that connection to snoop around your computer and retrieve or steal not just data, but perhaps also your user ID and password to gain access to websites you visit.

How You Can Protect Your Data

Below are some steps you can take to help you protect your data when you use Wi-Fi networks:

- As a rule, you should only connect to Wi-Fi networks that you absolutely trust. Make sure that your communication is secure, and disconnect the Wi-Fi network when you are done using it.
- Turn off shared folders. In some circumstances, hackers can reach into your PC and access information in shared folders.
- Run a comprehensive security suite and keep it up to date to prevent spyware and viruses.
- Beware of the information you share in public locations. Even seemingly innocuous logins to web-mail accounts could give hackers access to your more important data, especially if you re-use similar passwords for multiple online activities.
- Use a VPN when possible, and try to only visit HTTPS websites.
- Be sure that your home Wi-Fi network uses encryption, specifically WPA3 encryption if available. WEP is an older version of less secure Wi-Fi, as is the original WPA technology. Since 2006, all routers are WPA2 certified. WPA3 routers hit the market as of early 2018.

BLUETOOTH SECURITY

Devices can easily pick radio waves out of the air, so people need to take precautions when sending sensitive information over a wireless connection. Bluetooth has an automatic connection, which makes it more risky because it leaves you vulnerable to people trying to gain access to your information without your permission.

- Types of Bluetooth Attacks: Common ways that people attack you via Bluetooth is by sending you unwanted messages, accessing private information, or targeting outdated Bluetooth interface that allows the pairing of devices without the user's consent.
- Turn off Bluetooth: The best course of action is to turn off your device's Bluetooth feature after you have finished using it.

- Set to Undiscoverable: If a device is set to ‘discoverable,’ it will be constantly broadcasting its presence to other devices that can pair with it. The feature to set your Bluetooth on your device to ‘undiscoverable’ will be in “Settings” under the “Bluetooth” tab. Bluetooth accessories previously paired with your device will still connect.

Protect Yourself: Online Shopping

SHOP AT SECURE WEBSITES

The world of electronic commerce, also known as e-commerce, enables consumers to shop at thousands of online stores and pay for their purchases without leaving the comfort of home. Consumers expect merchants to not only make their products available online, but to make payments a simple and secure process. However, the same things can go wrong shopping online as in the real world. Sometimes it is simply a case of a computer glitch or poor customer service. Other times, shoppers are cheated by clever scam artists.

Secure sites use encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en-route. The only people who can unscramble the code are those with legitimate access privileges.

How to Tell When You are Dealing with a Secure Site

- If you look at the top of your screen where the Website address is displayed (the "address bar"), you should see https://. The "s" that is displayed after "http" indicates that Website is secure. Often, you do not see the "s" until you actually move to the order page on the Website.
- Another way to determine if a Website is secure is to look for a closed padlock displayed on the address bar of your screen. If that lock is open, you should assume it is not a secure site.

There are Some Clues to Look Out for to Determine Whether a Shopping Site is Fake

If any of these questions trigger a warning bell in your head, you will be wise to find another online merchant:

- Are there outlandish claims that you question?
- Do the company's prices seem unusually low?
- Does it look like the merchant is an amateur or the website design is horrible and hard to navigate?
- Are there a lot of spelling or grammar errors?
- Does the company's phone go unanswered?

- The use of a post office box might not send up a red flag, but a merchant who does not also provide the company's physical address might be cause for concern.
- What are the brand selections? If the seller claims to specialize in selling one product, but is also selling other products it may be a cause for concern.

Research the Website before You Order

- Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy.
- Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line.
- Call the phone number and ask questions to determine if the business is legitimate. Even if you call after hours, many companies have a "live" answering service, especially if they don't want to miss orders. Ask how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.
- You can also research a company through the Better Business Bureau, or a government consumer protection agency like the district attorney's office or the Attorney General. Remember, anyone can create a Website.
- Read reviews or history of online sellers. Be aware these are not always unbias.
- There are numerous websites dedicated to documenting a website's history, such as Who.is and Archive.org. If they say they have been in service for ten years, you can check the truthfulness.

Read the Website's Privacy and Security Policies

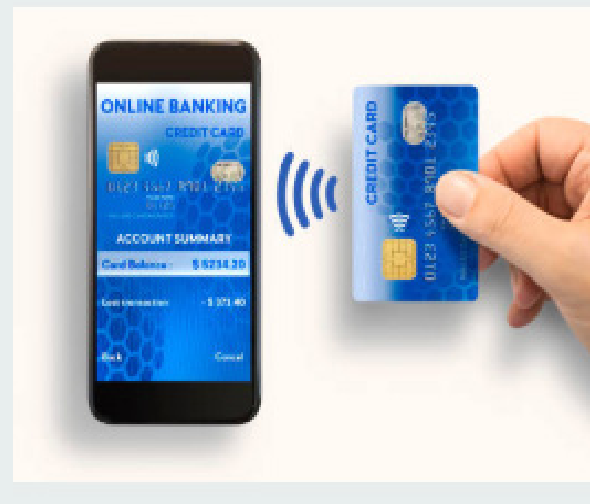
Many reputable online websites offer information about how it processes your order. It is usually listed in the section entitled "Privacy Policy." A website's Privacy Policy must detail:

- The type of information gathered. This would include an overview of what information is mandatory and what is optional. If the information is optional, it will disclose how it will be used.
- How the information may be shared or disclosed. If your information is shared, you can expect to receive "spam" (unsolicited email), and even mail or phone solicitations from these companies.
- The process to review and change the information they have on you.
- The policy's effective date and an overview of subsequent changes. The company can file for bankruptcy and sell its customer database. The Web merchant might be purchased by another company with a weaker privacy policy. And the company's data can be subpoenaed for law enforcement investigations or civil cases. You have little control over the use of your customer data in such matters.
- Be aware of General Data Protection Regulation (GDPR) - Europe's data protection law.

The online merchant's data security practices are also often explained in the Privacy Policy, or perhaps within a separate Security Policy.

- Look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related practices, such as:
- TrustArc (www.trustarc.com), Verisign (www.verisign.com), or BBBonline (www.bbb.org).

Be Aware of Cookies and Behavioral Marketing



- Online merchants as well as other sites monitor our shopping and surfing habits by using "cookies," an online tracking system that attaches pieces of code to our Internet browsers to track which sites we visit as we search the Web.
- "Persistent" cookies remain stored on your computer while "session" cookies expire when you turn the browser off. Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies, but the tradeoff may limit the functions you can perform online and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order.
- There are a number of companies that specialize in targeted online advertising called "behavioral marketing." Consumer information, such as browsing and search history, IP addresses, and cookies, are collected to create a dossier to generate relevant advertisements. Companies say this practice benefit consumers by being exposed to more targeted advertising, and that online merchants can make more money, more efficiently by targeting the right shoppers.

Payment Methods: What's Safest?

Typically, the safest way to shop on the Internet is with a credit card. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments of the disputed charges during a creditor investigation.

- When it has been determined that your credit card was used without authorization, you are only responsible for the first $50 in charges. However, if it was used online, you are not obligated to pay anything. Overall, you are rarely asked to pay this charge.
- Make sure your credit card is a true credit card and not a debit card, a check card, or ATM card. The protection on each type of card varies. Protections are strongest with bank-issued credit cards.

Do Not Use a Debit Card When Making Purchases Online

As with checks, a debit card exposes your bank account to thieves. Your checking account could be wiped out in minutes. Further, debit and ATM cards are not protected by federal law to the extent of credit cards.

Online Shopping by Check Leaves You Vulnerable to Bank Fraud

Additionally, sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase.

Beware of money transfer services, such as Western Union, MoneyGram, or PayPal

You could be transferring cash to a fraudster. Scammers will ask consumers to send them payment using a money transfer service such as Western Union or MoneyGram because they can get your cash fast and it's difficult to trace. Legitimate sellers normally do not ask consumers to send payment that way. Money transfer services should only be used to send money to people that you know well, not to unknown sellers of merchandise online.

- Avoid paying with a bank account, when using a money transfer service. It is safer to connect the payment through your credit card because you are still protected by the Fair Credit Billing Act. This method is actually safer because the seller does not have your credit card number, and if any false charges are made, you can dispute them.

Know What Rights Protect Your Payment Information

The Restore Online Shoppers' Confidence Act, P.L. 111-345, (signed December 29, 2010) makes it illegal for a company that sells goods or services online to give a consumer's credit card number (or other financial account number) to a third-party for sales purposes. This practice is known as "data passing." The Act prohibits a third-party seller from charging a consumer for any good or service, unless the seller:

- Clearly and conspicuously discloses the material offer terms.

- The third-party seller is not affiliated with the initial merchant.
- Receive express consent for the charge from the consumer. The third-party seller must obtain the full financial account number directly from the consumer. The initial online seller may not transfer a consumer's financial account number to a third-party seller.

The Act also regulates "negative option" plans. A consumer must give express, informed consent before being charged for goods or services sold online through "negative option" marketing, such as "free trials" that the consumer must cancel in order to avoid being charged. Companies that use negative option plans must

- Clearly and conspicuously disclose the material terms of the transaction before obtaining the consumer's billing information.
- Obtain a consumer's express consent before charging the consumer.
- Provide a simple mechanism to stop any recurring charges.

Never Give Out Your Social Security Number

Providing your Social Security number is never a requirement for placing an order at an online shopping site. There is no need for the merchant to ask for it. Giving out your Social Security number could lead to having your identity stolen.

Disclose Only Essential Facts When You Order

When placing an online order, there is certain information that you must provide to the web merchant, such as your name and address. Often, a merchant will try to obtain more information about you. Merchants may ask questions about your leisure lifestyle or annual income. This information may be used to target you for marketing purposes. It can lead to "spam" or even direct mail and telephone solicitations. Don't answer questions that aren't required to process your order. Often, the website will mark which questions need to be answered with an asterisk (*). If a company requires information you are not comfortable sharing, leave the site and find a different company to purchase the product you want.

Keep Your Password Private

Many online shopping sites require the shopper to log-in before placing or viewing an order. The shopper is usually required to provide a username and a password.

Never Reveal Your Password to Anyone

When selecting a password, do not use commonly known information, such as your birthdate, mother's maiden name, or numbers from your driver's license or Social Security number. Do not reuse the same password for other sites, particularly sites associated with sensitive information. The best password has at least eight characters and includes numbers, letters, and special characters.

Consider using a trusted password manager to store passwords. Password managers approved for work at GSA:

- dashlane.com
- lastpass.com
- 1password.com
- KeePassXC
- Google Sheets

Don't Fall for "Phishing" Messages

- Identity thieves send massive numbers of emails to Internet users that ask them to update the account information for their banks, credit cards, online payment service, or popular shopping sites. These phishing emails may state your account information has expired, been compromised or lost, and you need to immediately resend it to the company.
- Some emails sent as part of such "phishing" expeditions often contain links to official looking Web pages. Other times the emails ask the consumer to download and submit an electronic form.
- Make sure you are directed to a legitimate company or website when clicking on a link from an email. You can verify this by looking at the URL and validating you are dealing with the correct company.
- Remember, legitimate businesses don't ask for sensitive information via email. Don't respond to any request for financial information that comes to you in an email. Again, don't click on any link embedded within a suspicious email, and always call the retailer or financial institution to verify your account status before divulging any information.
- If you identify a phishing email, clicking 'Unsubscribe' will not stop the email spam. Instead mark the email as spam so subsequent ematils from that sender will go to your spam box.
- Don't simply trust the email from a credit card company. Call the company directly to verify the request.

Always Print or Save Copies of Your Orders

- After placing an order online, you should receive a confirmation page that outlines your entire order. It should include the costs of the order, your customer information, product information, and the confirmation number.
- Print out or save a copy of the web page(s) describing the item you ordered as well as the page showing company name, postal address, phone number, and legal terms, including return policy. Keep it for your own records for at least the period covered by the return/warranty policy.
- Often you will also receive a confirmation message that is emailed to you by the merchant. Be sure to save and/or print this message as well as any other e-mail correspondence with the company.
- Properly dispose of receipts by completely destroying them or erasing them. The information on the receipts can be used by identity thieves to get information about you.

Shop with Companies Located in the United States

When you shop within the U.S., you are protected by state and federal consumer laws. You might not get the same protection if you place an order with a company located in another country.

Pay Attention to Shipping Facts

Under the law, a company must ship your order within the time stated in its ad. If no time frame is stated, the merchant must ship the product in 30 days or give you an "Option Notice." This gives you an opportunity to cancel the order and receive a prompt refund, or agree to the delay. Here are key shipping questions to ask:

- Does the site tell you if there are geographic or other restrictions for delivery?
- Are there choices for shipping?
- Who pays the shipping cost?
- What does the site say about shipping insurance?
- What are the shipping and handling fees, and are they reasonable?

Learn the Merchant's Cancellation, Return and Complaint-Handling Policies

Even under the best of circumstances, shoppers sometimes need to return merchandise. Check the website for cancellation and return policies. Be sure to check for the following:

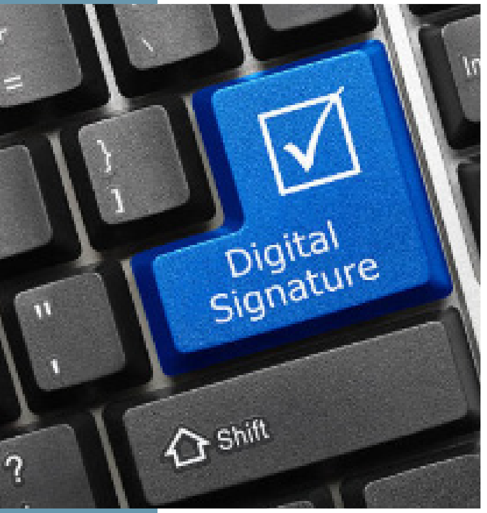
- Who pays for shipping?
- Is there a time limit or other restrictions to the return or cancellation?
- Is there a restocking charge if you need to cancel or return the order?

- Do you get a store credit, or will the company fully refund your charges to your credit card? If the merchant only offers store credits, find out the time restriction for using this credit.
- Does the merchant post a phone number and/or e-mail address for complaints?
- How long has the company been in business?
- Will they still be around when you need them?
- Is there an easy, local way for you to get repairs or service?
- Is there a warranty on the product, and who honors that guarantee?
- What are the limits, and under what circumstances can you exercise your warranty rights?

Don't expect less customer service just because a company operates over the Internet. This is especially important if you are buying something that may need to be routinely cleaned or serviced.

Be Wary of Identity Theft

As online shopping becomes more common, there will be more cases of identity theft committed over the internet. Imposters are likely to obtain their victims' identifying information using low-tech means like dumpster diving, mail theft, or workplace access to SSNs. But they are increasingly using the Web to apply for new credit cards and to purchase goods and services in their victims' names.



The same advice for avoiding low-tech identity theft applies to shopping on the Internet. Many are mentioned in the above tips. Most important: Be aware of who you are buying from. And use true credit cards for purchases, not debit cards.

Check your credit card bills carefully

Always check your bank for purchases you did not make. If you find some, immediately contact the credit card company and file a dispute claim.

Order your credit reports at least once a year

Order your credit reports annually, and check for accounts that have been opened without your permission.

- https://www.transunion.com

- https://www.experian.com
- https://www.equifax.com

More information: https://www.usa.gov/credit-reports

Consider Using Single-use Card Numbers

Consumers using some brands of credit cards can get "virtual credit cards," or single-use card numbers, which can be used at an online store. Virtual credit cards use a randomly generated substitute account number in place of your actual credit card number. They can also be used to buy goods and services over the phone and through the mail but can't be used for in-store purchases that require a traditional plastic card.

With this free service, you never need to give out your real credit card number online. Among the card companies offering it are Citibank, Bank of America, and Capital One. Citibank calls its virtual credit card offering a Virtual Card Account while Bank of America calls it ShopSafe. Capital One calls its tool Virtual Numbers from Eno. You can configure the expiration date and the maximum amount allowed for a virtual credit card. Once used, the card is tied to the merchant where the purchase was made, and cannot be used elsewhere.

A drawback to using a single-use card is returning items becomes a hassle because getting your money back is not clear. Being single-use, the money cannot be put back onto the card so you might have to accept a gift card or check in lieu. If you keep the receipt with the card number, it might ease the process.

Be Cautious with Electronic Signatures

An electronic signature, also known as a digital signature or eSignature, is any way of electronically signing an online document. The methods include signing with your finger, mouse, stylus, typing your name, checking a box, or any other method that verifies your identity, such as last four of your SSN.

Federal law enables shoppers to verify online purchases with merchants using an electronic signature. Usually, this process is nothing more than clicking on a box that validates you accept the terms of the order.

The Electronic Signatures in Global and National Commerce Act, also known as the E-Sign Act, is a complex law. It states electronic signatures and electronic records used in interstate and foreign commerce will not be denied validity just because they are in electronic form. Further, the law says online purchases do not need to be accompanied by the more traditional handwritten signature on a paper document.

Consumer advocates opposed the law because it lacks important safeguard against fraud. For example, the law does not require online merchants to comply with such standards as message integrity (security and accuracy in transmission), privacy of customer data, and authentication of sender.

The faults of the E-Sign Act require you to shop cautiously on the internet. The tips offered in this guide will help you make sure the online companies you choose are secure and honest.

Know How Online Auctions Operate

Online auctions connect buyers and sellers, allowing them to communicate in a bidding process over items for sale. Many people are drawn to online auction sites because they allow you to buy items at discounted prices. They offer a chance to sell some of your unneeded or unwanted possessions to raise extra money. For the most part, online auction sites are a safe way to exchange goods. But it makes sense to be cautious and aware.

The first step in safely using an online auction site is to read the terms of use, which will outline key issues such as whether or not the seller or the site is responsible for any problems that arise. Learn a site's return policy, as it may be difficult to return merchandise bought at auction. It's critical to check the policy, because you may be required to follow the seller's refund policy, rather than that of the auction site.

Once a consumer has agreed to a price with a seller, the buyer and seller arrange for payment and delivery of the product. Successful bidders can usually choose among several payment options, such as credit card, online payment service, debit card, personal check, cashier's check, money order, or escrow service.

If a seller requests payment in cash by private courier, or by check or money order through an overnight delivery service, you have a right to be suspicious. This could signal an attempt to commit fraud by taking your money without delivering the merchandise.

It always makes sense to pay by credit card because you'll have an option to seek a credit from the credit card issuer (also known as a "chargeback") if the product isn't delivered or isn't what you ordered.

To protect both buyers and sellers, some auction sites prohibit the use of wire transfers as a payment method. The Federal Trade Commission recommends that buyers do not pay by wire transfer because if something goes wrong, you are left with no refund and no recourse.

Another popular way to pay at auctions is with online payment services, such as PayPal. In this scenario, the buyer and seller set up accounts that allow them to make or accept payments. Buyers provide payment information, like bank account or credit card numbers, and sellers give information about where payments should be deposited. Some online payment services offer protection if the seller doesn't ship the goods.

Sellers can be scammed too. Fake check scams are the most common problem, although they can be avoided by not accepting checks, especially cashier's or certified checks, as payment, and by waiting to ship the goods until you get your payment in a reliable form.

If a buyer offers you a cashier's or certified check for more than the amount of the item, and asks you to wire the excess amount, don't do it. This it is a classic example of a fake check scam.

If you encounter a problem with a buyer or seller at an online auction site, such as eBay, it's important to report the problem to the site right away. You are probably not the only person being taken advantage of and you could help shut down illegal or unethical sellers by alerting the site to the problem.

Other common buyer complaints include sellers who do not deliver in a timely manner or fail to disclose relevant information about the product or terms of sale. You can also file a complaint to the Federal Trade Commission. Even though the FTC will not investigate individual claims, if it sees a pattern of law violations it can act against the seller.

Understand Your Responsibility for Sales and Use Taxes Online

The Supreme Court recently changed its ruling that online sellers had to collect sales tax if they had a physical presence in the state where the product was bought. Now, online retailers must collect the appropriate level of tax based on the buyer's state and local taxes.

Big online companies, such as Amazon, already collected sales tax for online purchases. However, small online businesses now must collect taxes on online purchases. Educate yourself on your state's online tax laws, so you don't pay more than you should.

Be Aware of Dynamic Pricing

Some online retailers use dynamic pricing to engage in price discrimination by charging different prices to different consumers for identical goods or services. When you purchase goods or services online, you may be paying a higher or lower price than another online customer buying the same item from the same site at the same time. While online shopping enables consumers to easily compare prices, it also allows businesses to collect detailed information about a customer's purchasing history and preferences. Online stores can use that information to customize the prices they charge you.

Amazon began experimenting with dynamic pricing in 2000. Different customers were offered different prices for the same product. Depending upon a consumer's purchase history and other information, Amazon might offer different prices matched to a customer's perceived willingness to pay a higher or lower price than the standard price.

While dynamic pricing has existed for a long time for time-sensitive products such as airline tickets, hotel room reservations, and rental cars, it's difficult to justify the use of dynamic pricing for goods and services that are not of a time-sensitive nature.

Online merchants can easily implement dynamic pricing by placing cookies on a customer's computer which will track a user's past interactions with the site. By using this information, sites can customize their interactions based on customers' past activities. Online stores can read the cookies on your browser to determine what products or services you searched for and bought, and how much you paid for them. This information helps them to predict how much you might be willing to pay for a product or service. In addition, click-stream technology allows a site to trace the path that a user follows as they view different pages on the site.

Some online stores may also consider other factors when determining pricing. For example, merchants might charge higher prices to customers who make repeated returns or demand extra service.

There are Several Ways that You May Be Able to Defeat Dynamic Pricing

Avoid logging in to a site before you obtain a price quote. Be sure to clear the cookies from your browser before you visit a site. Visit sites from different browsers (Internet Explorer, Firefox, Chrome, Safari, and others). Utilize price comparison sites that check prices from multiple vendors. Finally, if you do log in to a site, try leaving items in your shopping cart for a few days, to see if the merchant offers any discounts.

Avoid Shopping on Online Apps

Shopping apps have gained popularity for consumers for the ease and convenience. Your information, such as credit card details, are stored on these apps, in most cases all you have to do is click a button, and when you are ready to check out. Hackers realize this too, and can find vulnerabilities in an app's code in order to get your information or go on a shopping spree.

If you can't avoid using an app for shopping, there are ways you can protect yourself. First, go to official app stores like the Apple Store of Google Play. Fake or clone apps do exist for the sole purpose of eliciting your information. Read the reviews to make sure the app is legitimate.

Use the security protocols, if an app offers them. This can include password or PIN protection before making a purchase.

Protect Yourself: Social Media

SOCIAL NETWORKING DOS AND DON'TS

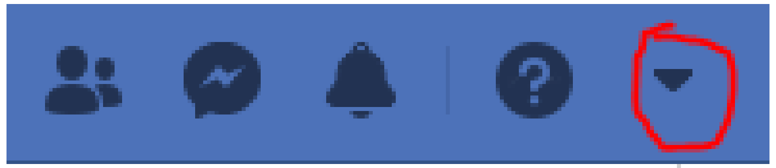
Social media is an easy way to stay connected to friends and family, but you should be wary of the information you publish on these sites and who can view the material on such sites. If you have a social media accounts, it is important to appropriately set up your account security settings, as well as limit certain types of information published on your account. Realize that even with correctly implementing your security settings, your information can still be used against you. Establish and maintain connections with people you know and trust; review your connections on a regular basis.

- Assume anyone can see information you post about your activities, location, and personal and professional life.
- Make sure your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face.
- Post pictures taken at a distance or angle that conceals your identity. Additionally, avoid posting pictures that gives away personal identifiable information (PII) such as license plates or addresses. Sophisticated users can use small clues to determine ID and location.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Facebook

In order to set up your Facebook security settings, click the question mark located on the top right of the page. A drop down menu will appear. First, start by clicking Privacy Check-Up. A box with three modules will appear on the screen. Go through each of the modules and set up the settings as desired. At a minimum, they should be set to 'Friends'.

Click on the arrow next to the question mark located in the top right of the page.

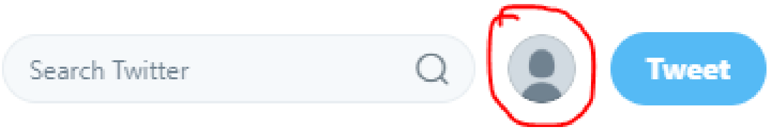


From the drop down menu, click Settings. Go thru the menu to the left, and continue going through the information and setting it up to your preferences. Important settings to format are

Timeline and tagging, Location, and Face recognition.

Twitter

In order to setup your Twitter account settings, click on more... A drop down menu will appear. Click on Settings and privacy.



Go through the options on the left side of the page, and set up the preferences as desired.

- Some important features to set up include 'Login and security', which is located in the **Account** option. In **Privacy and safety**, under settings, you can protect your postings, location, and personal data among other things.
- Regardless of your privacy settings, assume anyone can see information you post about your activities, location and personal and professional life. Furthermore, one you tweet, you cannot delete them.

LinkedIn

Limit the contact information you share on your profile by clicking your image in the upper right corner. Select View Profile from the menu. Scroll through the information and remove your phone number, address, or other contact information.

Limit other PII in your public profile. Click on your image in the top right corner and choose "Settings & Privacy" under the accounts tab. Choose **Edit Your Public Profile**. Click **Change**. Make any edits to your profile that may affect your privacy, and then hit save.

Review your privacy control settings. Go to **Settings & Privacy** > **Privacy** > **Profiling viewing options**. Set it as desired.

Instagram

- Go to your Instagram profile, and click **Edit Profile**, in the top middle of the page. This will bring up all your Instagram account settings.
- Go to **Privacy and Security**. Toggle on **Private Account**, if you have not already done so. Toggle off **Show Activity Status**, if you have not already done so.
- Go through the remaining options of this page, and set it up as desired. Another way to make your account more secure is to setup the two-factor authentication, which is also an option on this page.

Snapchat

More people are turning to Snapchat because messages, also known as Snaps, only last for a 24-hour period. However, strangers can still view these messages, especially if you do not have your security settings setup correctly.

- Make sure only your friends can contact you. Access your settings from your profile tab. Look for **Contact Me** option under **Who Can** heading, and set it to **My Friends**.
- Select who can see your story. Go to your settings, scroll down to **Who Can** section and tap **View my Story**. At a minimum, you should select **My Friends**.
- Hide yourself from the 'Quick Add' section. This feature enables you to be seen on friend of friends list of suggested users to add. Go to settings, scroll to **Who Can**, and tap **See Me in Quick Add**, and turn it off.
- Use "Ghost Mode" to hide your recent locations. Tap the gear icon, turn on **Ghost Mode**, then choose "Until Turned Off."

Protect Yourself: Computer Security

ANTIVIRUS

Making sure your computer is protected is a crucial step to protecting your identity. The best place for a thief to look is in through a computer where personal information is stored. The more safeguards you set up the more difficult it will be for an impostor to access your personal data.

Get an Antivirus Program:

An antivirus program is designed to search for, prevent, detect and remove software viruses. These programs focus on internal attacks like malicious file. You can purchase different antivirus software that can:

- Schedule scans to automatically run for you.
- Initiate scans of specific files, flash drives or CDs at any given time.
- Scan certain directories or files for known malware patterns.
- Display the "health" of your computer.
- Remove malicious codes that were found.

There are many different antivirus programs available for purchase. There isn't a one-type-fits-all program. Therefore, some things to consider when selecting an antivirus program include:

- Is the service reliable? A reliable program should not conflict with other protection programs installed on your computer. It should regularly update in order to provide up-to-date protection. It should allow you to automate scans.
- How will the antivirus program impact the performance of your computer? A program shouldn't have too much influence on the startup or routine processes of your computer.
- What is the level of usability of the program? Many people aren't knowledgeable about the inner workings of antivirus software. With that being said, a program shouldn't leave you hesitant in testing the features of a product. Additionally, you should be able to know the full potential of the program. Antivirus programs exist for every level of a user's technical experience.
- What is the reputation of the antivirus program? It may seem intuitive, but good programs are well known. Read reviews and shop around. Be wary of antivirus programs that are not well known. They could be malware disguised as antivirus software.

Free antivirus programs also exist. These programs typically do not come with the special features, such as child settings, which come with paid antivirus programs. However, these free programs usually are up-to-date with the latest malware and their scanning performance is comparable to paid programs.

Use a Firewall:

A firewall is a piece of hardware or a software program that helps keep out viruses, worms and hackers from your computer that are contracted over the Internet. The main difference between a firewall and antivirus software is the main function of the firewall is to stop malicious software from infecting your computer. Theoretically, if you have a good firewall you would not need antivirus software, but it's always good to be doubly secure. Microsoft recommends protecting every computer even if you have more than one connected at home or in an office network.

Consumers should have a hardware firewall to protect your network (e.g. a router) and a software firewall for each computer. Both forms of protection help stop a spread of a virus to your whole network if one of the computers becomes infected.

Keep Operating System (OS) Updated:

Updates from vendors are important and used to fix any security holes that could be present in the OS, and all hardware and software. Using updates keeps your system up to date and installs the latest security functions.

If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities.

Don't buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to "break and enter" your computer.

You can check to see if your computer is up to date by:

- Clicking Start and then All Programs and selecting Windows Update
- On the left side, select Check for Updates
- If any updates pop up, click Install Updates
- Proceed to enter in the appropriate password if asked

For Windows 10:

- Clicking Start and then Settings and selecting Update and Security
- Select Check for Updates
- If any updates pop up, click Install Updates

- Proceed to enter in the appropriate password if asked

Steps to set up automatic updates for Windows:

- Open Microsoft Internet Explorer internet browser
- On the right side of the page, Internet Explorer will display the current status of the update if it is already set up
- If it is not already set up, click Turn on Automatic Updates
- In the window, select OK

Password-Protect Guest Accounts

PC's generally allow you to have accounts, one for the main administrator and one as a guest account. Set up a password for all accounts, even the guest one. You don't want someone to log onto the guest account and set a password so you no longer have access to it. This can easily provide extra precautions to your PC.

Encrypt Sensitive Information

Encrypting your information makes it harder for hackers to access, gain, and copy data. Ensure you give personal information over encrypted websites only.

If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the "s" is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Some websites and social media sites will allow users to change the settings to "Always use HTTPS". Check the site settings to see if this is an option.

Windows allows you to encrypt or decrypt folders or files by:

- Right-clicking the desired file or folder to encrypt
- Select Properties
- Click on the General tab and select Advanced
- Check the box that is labeled Encrypt contents to secure data

- To decrypt, uncheck this same box
- Select OK

Back Up Your Files

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

Download or Update from the Official Company

Go directly to the company's website when installing or updating software. Pop-ups might appear stating you need to update or download new software, but the link could lead to an illegitimate source, which could make yourself vulnerable to an attack.

Don't click on pop-ups that say you have a virus on your computer. Open your antivirus program via your Start menu, and run a scan from there.

Use Strong Passwords and Change Them Regularly

- Strong passwords are necessary for any type of electronic devices, not only PCs.
- Here are a few principles for creating strong passwords and keeping them safe:
- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
- Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or dictionary words.
- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts. This is the same as directly connecting accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam.
- Keep your passwords in a secure place, out of plain sight.
- Use password managers like:
  - dashlane.com
  - lastpass.com
  - 1password.com
  - KeePassXC

- Google Sheets

COOKIES: LEAVING A TRAIL ON THE WEB

What is a Cookie?

A cookie is information a site saves to your computer using your web browser. Not all cookies are created equal and not all of them are bad. Most cookies allows sites to record your browsing activities – like what pages and content you've looked at, when you visited, what you searched for, and whether you clicked on an ad. However, there are some cookies tell websites whether you are logged into a specific computer.

Data collected by cookies can be combined to create a profile of your online activities.

Who Places Cookies on the Web?

First-party cookies are placed by a site when you visit it. They can make your experience on the web more efficient. For example, they help sites remember:

- items in your shopping cart
- your login name
- your preferences, like always showing the weather in your hometown
- your high game scores

Third-party cookies are placed by someone other than the site you are on. These may include an advertising network or a company that helps deliver the ads you see. They may be used to deliver ads tailored to your interests.

Managing Cookies

Various browsers have different ways to let you delete cookies or limit the kinds of cookies that can be placed on your computer. When you choose your browser, you may want to consider which best suits your privacy preferences.

To check out the settings in a browser, use the 'Help' tab or look under 'Tools' for settings like 'Options' or 'Privacy.' From there, you may be able to delete cookies, or control when they can be placed. Some browsers allow add-on software tools to block, delete, or control cookies. And security software often includes options to make cookie control easier.

If you disable cookies entirely, you may limit your browsing experience. For example, you may need to enter information repeatedly, or you might not get personalized content or ads that are meaningful to you. However, most browsers' settings will allow you to block third-party cookies without also disabling first-party cookies.

Flash Cookies

A Flash cookie is a small file stored on your computer by a website using Adobe's Flash player technology.

Flash cookies use Adobe's Flash player to store information about your online browsing activities. Flash cookies can be used to replace cookies used for tracking and advertising, because they can also store your settings and preferences. When you delete or clear cookies from your browser, you won't necessarily delete the Flash cookies stored on your computer.

Controlling Flash Cookies

Most likely your browser will not support the option of disabling Flash cookies. To delete Flash cookies go to Adobe's Website Storage Settings panel. There, you can view and delete Flash cookies, and control whether you'll allow them on your computer.

Like regular cookies, deleting Flash cookies gets rid of the ones on your computer at that moment. Flash cookies can be placed on your computer the next time you visit a website or view an ad unless you block Flash cookies altogether.

"Opt-Out" Cookies

Some websites and advertising networks have cookies that tell them not to use information about what sites you visit. These types of cookies are used for targeting advertisement.

You can download software – an "add-on" to your browser – that controls whether and how cookies – including opt-out cookies – are stored or deleted. You can find add-ons on sites sponsored by the browser. Look through the settings or "Help" function. Browser companies review most add-ons for security and functionality before making them available for download, but as with any software, don't download an add-on unless you have checked it out and trust the source.

Programs from the online advertising industry, including The Network Advertising Initiative and the Digital Advertising Alliance, offer tools for opting out of targeted advertising often by placing opt-out cookies – offered by their members. You also can opt out by visiting advertising networks and advertiser websites one by one.

Deleting all your cookies will erase any opt-out cookies you've downloaded. To restore opt-out cookies, you will have to go through the opt-out procedure again.

Keep your Browser Up-to-Date:

No matter which browser you use, it's important to keep it updated. An out-of-date browser can leave your computer vulnerable to attack by malware, which could intercept sensitive data like your logins, passwords, or financial information. Most browsers update automatically, or prompt you to update to the latest version.

PRIVATE BROWSING

Private Browsing

Many browsers offer private browsing settings that are meant to let you keep your web activities hidden from other people who use the same computer.

With private browsing turned on, your browser won't retain cookies, your browsing history, search records, or the files you downloaded. Privacy modes aren't uniform, though; it's a good idea to check your browser to see what types of data it stores. Although it won't keep cookies **after** the private browsing session ends, cookies used **during** the private browsing session can communicate information about your browsing behavior to third parties.

NEW TECHNOLOGIES

Other Tracking Technologies:

- New technologies are constantly emerging, and some can be used to track your online activities even if you control regular cookies. These are generally referred to as "supercookies" or "permacookies". If companies offer you an "opt-out", they need to respect your preference, whether they use supercookies or regular cookies.
- Another type of cookie to look out for is the "zombie cookie". Zombie cookies are when third party cookies are placed outside of your browser's designated cookie storage. In order to prevent zombie cookies, you have to delete the cookie that is reinstalling the third-party cookies.

"Do Not Track" Tool

- Do Not Track is a tool that allows you to express your preference not to be tracked across the web. Turning on Do Not Track through your web browser sends a signal to every website you visit that you don't want to be tracked. Companies then know your preference. If they have committed to respect your preference, they are legally required to do so.
- Some browsers already support Do Not Track. If you want to use Do Not Track, check to see if the browser you use offers it – or use a browser that does.

Protect Yourself: Internet of Things

WHAT IS AN INTERNET OF THINGS DEVICE?

Modern day advances have made all devices "smart" devices. People fill their homes with smart devices in order to create an ease of living. This can include anything from "smart" refrigerators to lightbulbs. Most times all it takes to control these "smart" devices is downloading an app and operating it from your phone. However, any time you connect anything to the internet, you are open to attacks and collection of personal information. Therefore, it is important to know how best to protect yourself if you use these devices.

The Internet of Things (IoT) refers to physical devices connected to the internet in order to collect and share data. Because of cheap processors and wireless networks almost anything can be part of the IoT. If it can be connected to the internet and controlled using the internet, it is considered to be an IoT device. IoT devices often refers to devices where connectivity is not standard, which excludes desktops, laptops, tablets, and smartphones.

The Scope of IoT

The cost of adding sensors and an internet connection to devices continues to decrease. Therefore, the amount of IoT devices continues to grow. According to Gartner, a technology research company, in 2020 the amount of IoT devices will reach 20.4 billion.

The biggest consumers of IoT devices are North America, China, and Western Europe. According to International Data Corporation (IDC), in 2019, the worldwide spending on IoT is set to reach $745 billion, an approximate 15.4 percent increase from 2018.

In 2016, 38 percent of companies in a Tech Pro Research survey said they are using IoT devices, while 30 percent say they are in the planning or considering stage of adopting IoT devices.

The importance of these numbers show, even if you do not plan on utilizing IoT devices, you may not be able to totally avoid IoT devices. If you use the services of companies, such as energy and health care companies, they may use IoT devices and services. Consequently, you could still be vulnerable to your information being collected.

IoT Privacy

IoT devices are full of sensors constantly collecting data about you. These devices can capture an explicit view of your pattern of life. Imagine your smart coffee pot is programmed to start when you wake up, your thermostat is programmed to decrease the temperature while you are working, and your smart refrigerator tells you to buy more milk. That is just a snapshot of the full extent of information that can be collected. While not all companies collect this data, many companies that collect the data use it for marketing purposes. Hackers and other nefarious actors seek to exploit this data, unbeknownst to the user.

The best way to understand the privacy of your devices is to read the privacy policies of the company or product. It will outline what they are collecting and what they do with the data.

Overall, when it comes to data privacy, you are at the mercy of the company. In order to use the device, you must accept the company's terms. Users must decide if allowing IoT devices on their home network is an acceptable risk to them. The other option is to completely opt out of IoT use altogether.

IoT Security

IoT devices are full of sensors constantly amassing sensitive data about you. Unfortunately, IoT security has been very poor. Many times, companies neglect the thought of basic security features for these devices, such as encryption of the data.

In addition to collecting personal data, hackers use IoT devices as a means to take advantage of network vulnerabilities. This means hackers can gain access to other devices on the same network, such as PCs or phones, which are more likely to hold valuable data.

How to Protect Yourself

- Change the default password. IoT devices are typically programmed with a default password. Avoid any IoT devices or systems that do not allow you to change the default password. Hackers may have knowledge of these devices and may be able to use the passwords to gain control.
- Update your devices. Just as you should with non-IoT devices, you should keep IoT up-to-date with the current version. One of the purposes of updates is to patch vulnerabilities in the devices so hackers cannot gain access to the devices. Do not use or purchase IoT devices that do not offer updates.
- Use an IoT scanner. IoT scanners are in the infancy stages, but they can still discover weaknesses in device security. These scanners will check if your IoT devices can be found publically, which exposes them to potential hackers. This service will scan your security cameras, baby monitors, smart TVs, and wearables. Be sure to research the validity of these types of scanners.

Things to Consider

- How connected do you need to be? While it may ease certain aspects of your everyday schedule, ask yourself if you need an IoT device. Remember the more devices you have connected, the more ways there are for hackers to get your personal information.
- Be aware there are some products you would not expect to need an internet connection.
- The only way to absolutely protect yourself from IoT vulnerabilities is to *not* use the devices and services.
- IoT devices that cannot be updated should be discarded.

Protect Yourself: Social Engineering

CLICKBAIT

"Social Engineering" is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. This includes a wide range of methods across a wide range of media, including both online and in-person interactions. The strategies used by actors engaged in social engineering focus on using deception to collect information while disguising the means of collection. Targets range from individuals to organizations, both public and private, and actors may be criminals, terrorists, or agents of foreign governments.

"Clickbait" is a link designed to entice users to click it and read, view, or listen to the linked piece of online content. Clickbait commonly appears as news articles, interactive media (i.e. quizzes, games, etc.), or advertisements promising some kind of reward. In some instances these links can be benign; however they often serve as a means of collecting personal information or delivering viruses. Beyond cataloging your interests, some links may request accesses or permissions, while others may obtain information from you in the form of a fun quiz.

How to Defeat Clickbait

- Mouse over the link to determine the linked website, if you do not recognize the URL do not click the link.
- Carefully read any prompts and avoid providing any personal information or permission to access your information.
- Some web browsers offer extensions that filter out or identify Clickbait content.
- You can report deceptive links to the website administrator, though some sites do not have restrictions on Clickbait.

Phishing

Phishing is an attempt to acquire information such as username, password, pin, account number, and credit card details, by masquerading as a trustworthy entity in an electronic communication. When in doubt, examine the message for clues to its authenticity!

How Can I Avoid Being the Victim of a Phishing attack?

- Take the time to carefully read emails that request any type of information from you, in order to determine their authenticity.
- Be careful of divulging Personally Identifiable Information (PII) in email form

unless the recipient has been verified and the message itself is properly protected (encryption).

- Contact the service desk, or your internet service provider directly utilizing previously tested methods (saved phone numbers, Global Address List) if you receive email messages requesting account information (contact information provided below). As a matter of policy, most legitimate entities will never ask for your account information, username, pin or password in an email message.
- Be suspicious of unsolicited messages that seem “custom tailored” to you and your role within the organization (Spear Phishing), or are not digitally signed.
- Do not open or forward chain emails or strange offers. Not only does this expose other users to phishing attempts, it also causes unnecessary traffic on internal government networks, which can degrade performance.
- Input information into any form fields, either within the message or at any site to which the message links, unless you have verified the site and the source.
- Auto-forward email between your personal and government accounts. Not only is this dangerous from a phishing perspective, it is also prohibited by the Acceptable Use Policy (AUP).

If you receive an email that is obviously inappropriate for government systems, or if you believe that you have been the target of a phishing attempt, please conduct the following immediately:

- Send the email as an attachment to Cybersecurity and Infrastructure Security Agency (CISA) at phishing-report@us-cert.gov, so that analysis can be conducted on the message to determine its nature, and to enable us to block messages from those malicious sources in the future.
- Contact the PENTCIRT (24 Hours) by phone: (703)695-2478 or by email: OSD.report.phishing@mail.mil to report the phishing incident.

IN-PERSON SOCIAL ENGINEERING

In-person methods depend largely on impersonation. This method often requires more specific targeting than others due to the level of involvement on behalf of the perpetrator. The actor may be seeking specific or protected information such as trade secrets. They will capitalize on complacency and elicitation techniques to collect or gain access to the information they want.

How Do I Protect Myself/Detect In-Person Social Engineering?

- Be aware that people, organizations, and nations may want information you have or have access to.
- Know the sensitivity of information being requested from you.

- Know if you have the authority to disseminate that information, and if the requester has the need to know.
- Exhaustively identify the requestor and their purpose.
- Always verify.

What to Do if You Think You May Have Been the Victim of In-Person Social Engineering.

- If you believe your personal information was compromised, file a police report and monitor your accounts.
- If you believe your organization’s information was compromised, contact your security department.
- Do not delay. Timely reporting and review of accounts will be the best mitigation for compromised information.

Remember ...

Having the latest operating system, software, web browsers, anti-virus protection and applications are the best defenses against viruses, malware, and other online threats. Do not take links at face value. Link text and appearance are easy to make obsure. Always verify any request for your or your organization’s information.

Protect Yourself: Junk Mail

HOW YOUR INFORMATION GETS ON THE JUNK MAIL LISTS

People are bombarded with unwanted advertising of one sort or another that arrives in a postal mailbox or email inbox. Facing significant declines in first-class mail volume, the United States Postal Service (USPS) is making deals with businesses to increase the volume of "standard mail", the USPS's official term for junk mail. While at first glance, junk mail is just a minor annoyance, it can be dangerous. For example, you can overlook important mail, fall for scams, and be subject to identify theft from applications sent to you.

- Junk mail is the result of direct mail companies sending catalogs, solicitations, coupons, flyers, and applications because of an agreement made with the USPS for reduced postage rates.
- These mail companies are not attracted to sending mail to random people who have no interest in their products. Therefore, mailing lists are created from information about your past purchases and interests. The information can come from public records, phone directories, club memberships, and other sources. Then mail companies will rent or buy these lists.

Dangers of Junk Mail

Junk mail is a nuisance and often gets thrown in the trash. But this is a dangerous because some of this junk mail might carry personal information that can be used against you. Criminals can figure out your buying trends and target the platforms you use to steal your information.

Pre-approved credit card offers or applications are especially dangerous. Identity thieves can steal these offers and apply for the credit card with your information. Sometimes these applications have some of the fields already filled with your information, which makes it easier for criminals to fill out the remaining fields.

In addition to credit card applications, some retail companies and other organizations will send documents with a barcode. Typically, this barcode contains information about you, and criminals can either extract that data or they can buy whatever products or services being offered in your name.

When you receive junk mail, the best method to combat negative consequences is to shred all of it. You might think it doesn't hold any value or personal information, but in the long run, criminals can create an extensive diossier of your information and buying habits.

Junk Mail Opt Out

Another way to stop the junk mail and advertisements is to use various opt out services.

While, using these services may not stop you from receiving all junk mail; it will only stop the mail companies registered to that service. Additionally, by opting out, you might opt out of mail that keeps you in-the-know about new products, services, and local deals.

Junk Mail List Removal

Data Marketing Association's (DMA) Choice Program is the first step to be taken off as many national mailing lists as possible. DMA Choice divides direct mail into four categories: credit offers, catalogs, magazine offers, and other mail offers. Within each category, you can request to start or stop receiving mail from individual companies. Or you can stop receiving mail from all companies you haven't purchased from or donated to within an entire category. DMA also offers email preference service, telephone preference service, and a do not call list for caregivers.

- If you have purchased, subscribed, or donated to a company, you will need to ask them DIRECTLY to be removed from their mailing list. Their contact information is included on the DMA site.
- The changes should take effect 90 days after your request was submitted because some mailings are prepared in advance.
- There are two ways to opt out:

  Register Online. You may sign up online at the DMA Choice website. There is $2 processing fee for online registration. This is valid for 10 years. Visit https://dmachoice.thedma.org/register.php

  Register by Mail. Send the DMA Choice Registration Form (available at https://dmachoice.thedma.org/prefill_mailin_registration.php) plus a $3 processing fee. Send your check or money order to:

  DMA Choice
  DMA
  PO Box 900
  Cos Cob, CT 06807

  Register Names of Deceased. The Direct Marketing Association also gives you the ability to register the names of deceased loved ones with their Deceased Do Not Contact list (DDNC) at http://www.ims-dm.com/cgi/ddnc.php.

Catalogs, Mail Order Lists and Magazines

When you buy something from a mail order catalog, your transaction is likely to be reported to Abacus. Abacus members, mostly catalog and publishing companies, contribute and exchange information about their customers. Your name may also be sold to other catalog and publishing companies. When you ask for one catalog, you're likely to get catalogs from other companies as well.

There are two ways to opt out of the Abacus markerting database. You'll need your name, including any middle initial, your current address. If you move or change your name, you'll need to opt out again with your new address or name.

By Email: optout@epsilon.com

By mail: Epsilon
Attention: Privacy
P.O. Box 1478
Broomfield, CO 80038

* As a DMA member, Abacus subscribes to and suppresses any name and address on the DMA's Mail Preference Service file from its direct mail marketing lists

Another resource to opt out of catalogs is https://www.catalogchoice.org/ However, you have to opt out of catalogs one at a time; there is no list to stop all catalogs being sent to you.

Companies not Participating in the DMA and Abacus Opt-out Programs

Must be contacted directly. This includes magazines, charities and many professional associations. Usually you can find a toll-free customer service number and/or address on the advertising piece. Let them know you not only want to be off their list, but you don't want them providing your contact information to other companies.

For magazines, it is best to inform them that you do not want your name and address sold to others when you subscribe. Be sure to inform them in writing.

Opt-out of Credit or Insurance Offers

OptOutPrescreen.com was created by the major credit card bureaus and allows you to either opt out for five years or permanently. By completing this process your name will be removed from lists supplies by the Consumer Credit Reporting Companies, Equifax, Experian, Innovis, and TransUnion.

- Five Year Opt Out: To opt out of these offers for five years, go to https://www.optoutprescreen.com and click "Click Here to Opt-In or Opt-Out" at the bottom of the page. Then choose "Electronic Opt-Out for 5 years", and fill out the form and hit "Confirm".
- Permanent Opt Out: In order to opt out permanently, go to https://www.optoutprescreen.com and click "Click Here to Opt-In or Opt-Out" at the bottom of the page. Then choose "Permanent Opt-Out by Mail". Complete the online portion and click "Confirm". After, it should bring you to the Permanent Opt-Out Election Form. You must submit that with a signature to be opted out permanently.

After completing the form, it will take about five business days for the request to go through. You might continue to get offers for the next several weeks. Those are coming from companies that already accessed your information.

Opting out of Telemarketing

To stop receiving unwanted telemarketing calls, put your phone number on the National Do Not Call Registry. Visit https://www.donotcall.gov and click "Register Your Phone". Registrations do not expire, so if you have not previously registered click the orange button that says "Register Here". You can enter up to three phone numbers, and one email address. A verification email will be sent to that address and you must be able to click on the link that is sent to complete the registration.

- You can also register by calling 1-888-382-1222 from the phone you want to register. It's FREE.

It's important to remember that the Do Not Call rules do not apply to every telemarketer. Non-profits, charities, political organizations, polling companies, and anyone you have done business with recently. The Do Not Call Registry also won't stop scammers who are operating illegally or committing fraud (if they're already criminals, the Do Not Call list won't deter them). After your number has been on the registry for 31 days and you continue to receive calls you can file a complaint against someone who violates the Do Not Call list by calling the Consumer Complaint Center at: 1-888-225-5322 (888-CALL-FCC). You can also complain online at http://www.fcc.gov/complaints.

Flyers and Advertising Supplements

Flyers are those ads stuffed in with other advertisements and delivered to your mailbox. Envelopes containing an assortment of ads are another in this category, as are card decks which are a group of post-card sized bundles of advertising on card stock. The ads are often from local merchants and may be for carpet cleaning, window replacement, restaurants, cheap electronics and any number of other products and services. They are usually addressed to "resident" or "occupant" at your address.

To reduce this kind of junk mail, do the following:

- Look for a mailing label attached directly to the flyer. You may see the name of the distribution company near your mailing address. If you don't find a label, you may find a phone number printed on the edge of the flyer itself.

- Contact the company as indicated below, and request that your address be taken off the mailing list. If you're making a written request, send a copy of your mailing label along with the letter. If you call, chances are you'll have to work through a telephone tree and leave your name and address on an answering machine. It usually takes at least four to eight weeks to be removed. In some cases, the company may have a website that will allow you to remove yourself from their lists.

These are the major residential or occupant mailers:

- RetailMeNot Everyday. You can remove your name and address from RetailMeNot Everyday (Redplum) mailings by completing the form at: https://www.retailmenot.com/everyday/unsubscribe
- Val-Pak Savings Coupons. Val-Pak maintains regional lists, not a central one. Send your request to the address printed on the envelope you receive. If you receive the blue envelope you can also remove your address from their website at: https://www.valpak.com/coupons/show/mailinglistsuppression

You may have to notify the distribution company more than once to make sure that your address has been removed from the mailing list. Once your name has been removed from the company's mailing list, you are also likely to have to remind your postal carrier not to deliver the advertising flyers.

Protect Yourself: Information Brokers, Data Brokers, & Data Vendors

A growing number of websites sell (or give freely) personal information of individuals. These online information brokers (also known as data brokers or data vendors) gather personal information from many sources including white pages listings, publicly-available sources, and public records. Some information brokers also offer the ability to conduct "social searches", which gather information by searching public profiles on social networking sites.

Types of information available via these databases may include:

- Full name
- Physical address
- Marital status
- Telephone number
- A wide range of other information: Date of birth, how much you owe on a mortgage, the ages of your children, etc.

Information brokers may offer the ability to look someone up via their name, email address, telephone number, or Social Security number. Much of the information sold by online information brokers are gathered through public records. This may include portions of DMV records, court records, birth certificates, marriage certificates, death certificates, property records, arrest and conviction records, and even voting records. The extent of information available in public records will vary from state to state and county to county.

Data vendors are prime targets for hackers because of the personal data stored on their databases. It is not only important to limit your presence on these databases, but to monitor your personal and financial information via certain monitoring groups.

Restricting Access to Personal Information

There is no single mechanism of suppressing your information from all information broker databases at once. However, there are a number of measures you can take to make this information more difficult to collect or retain.

Opt Out of Prescreened Credit and Insurance Offers

Many companies that solicit new credit card accounts and insurance policies use prescreening to identify potential customers for the products they offer. Prescreened offers - sometimes called "preapproved" offers - are based on information in your credit report that indicates you meet criteria set by the issuer. Usually, prescreened solicitations come via mail, but you also may get them in a phone call or in an email. If you decide you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt out of receiving them for five years or opt out of receiving them permanently.

- To opt out for five years: Call toll-free 1-888-5-OPT-OUT (1-888-567-8688) or visit www.optoutprescreen.com. The phone number and website are operated by the major consumer reporting companies.
- To opt out permanently: You may begin the permanent Opt-Out process online at www.optoutprescreen.com. To complete your request, you must return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

Opt-Out of Data Broker / Data Vendor Web Sites

Though not required to do so, some information brokers offer a method to opt-out. Some will require detailed personal information (such as a state-issued ID) to identify a consumer before suppressing the information from their databases. You will have to decide for yourself if you are comfortable providing them with this information. Please be aware opting out may be a fruitless endeavor, as companies could re-post your information at a future date, making it necessary for you to check back to see if your information has been reposted and then repeat the opt out procedure.

If you choose to opt yourself out of the online information brokers, note these tips:

- Conduct some research to see what records each data broker/ vendor has collected about you and your family.
- Some data brokers/vendors may have information about you and your family under multiple listings; you will need to repeat all the steps for the removal process for each listing.
- Follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator. Detailed steps are provided below.
- Encourage family members and other cohabitants to remove their records from data aggregators as well (their information can repopulate your information).

Unsolicited Commercial Mail Five Year Opt Out Procedures

The Direct Marketing Association's Mail Preference Service allows you to Opt-Out from receiving unsolicited commercial mail for five years. (www.dmachoice.org)

To Opt Out of Credit Offers, Catalogs, Magazines, Other Mail go to www.dmachoice.org

- Click "Get Started" on the upper right of the screen. Fill in all required information. Be sure to add all addresses you've lived at for the last 5 years. Don't forget to use your generic email address. Click the link provided.
- On the page that comes up, click "log in", use your generic email as Log In name. Click in to all 4 categories and choose what you do / do not want to receive in your mail.

By opting out of "Catalogs", "Magazine Offers", and "Other Mail Offers", you are ONLY opting out via this site from NEW companies from using lists to send you offers. If you are receiving magazines, catalogs and/or other mail from companies you've utilized previously, then you must contact each individual company to request opting out of their products.

National Email Opt-Out Service

This email preference service allows the removal of email addresses from National Lists.

- Go to https://www.ims-dm.com/cgi/optoutemp.php
- Under "More than just mail" (in the middle of the page) click "Email Opt Out Service."
- Type up to 3 of your email addresses in the spaces provided.
- Enter the security numbers and/or letters in the space provided, click "Submit."
- Go to each of the email addresses you entered and click the verification link provided.

What to Look For on Data Broker/Data Vendor Websites

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames.

Once you have located information you want removed, you should save your findings to facilitate the removal process.

The information presented about how to remove personal details from data brokers / vendors is subject to change.

Data Broker / Data Vendor Opt-Out Procedures

There are approximately 264 data broker and data vendor websites. The below procedures are just a sampling of the data broker and data vendor websites and their own particular opt-out procedures. For a comprehensive list of most of the data broker / vendor websites visit:

https://www.privacyrights.org/data-brokers

Prior to the start of the Opt-Out process create an email address you will use only for the sole purpose of this process. Once completed you will “burn” or not use this email address again.

Remember, DO NOT use personal information or PII in the creation of this email address. This is a generic, non-secure, email address many of the Websites will require you enter to “validate” your identification.

Remember when checking this generic email account throughout your Opt-Out process to look in the “Junk Mail” folder; sometimes verification emails will be diverted to this folder instead of your inbox.

PeopleSmart, www.peoplesmart.com

- Go to the bottom of the page. Under “Members” click “Opt Out”.
- Type the appropriate information in the given boxes focusing on First Name, Last Name, Pick a State You Live or Have Lived in.

  Click “Find My Listing”.
- If you information is listed, click the box.
- Enter your email address and click “Send Verification Email.”
- Go to your email and click the link that was sent to you.

USA People Search, https://www.usa-people-search.com/manage/

- Enter your First Name, Last Name, and All States. Click “Find My Listing.”
- If you’ve located your entry, click “That’s The One”.
- Click “Continue” on the next page.

Intelius, www.intelius.com

- Scroll to the bottom of www.intelius.com and click “Privacy Policy”.
- Scroll down to “3. Updating or Removing Your Information” and in section “b. Intelius and US Search” locate “click here for you options”

  Click “click here”

  Enter your First Name, Last Name, and State.

  If you’ve located your entry, click “Select and Continue”.

  Enter in your email, and click the verification link provided in your email.
- Intelius owns, or is affiliated with, the following people search websites: Zabasearch, Public Records, Spock, iSearch, PeopleLookUp, Phonebook, DateCheck, LookupAnyone, Peoplefinder, USSearch, and Anywho.
- Wait the maximum 72 hours for all of your personal information to be removed. After 72 hours, search for your information on all of the sites again. If your personal information is still found; resend your Opt-Out request.

MyLife, www.mylife.com

- First do a search of yourself prior to emailing. You can create a profile, see what personal information is available and then delete the profile.
- Email MyLife via email at privacy@mylife.com.

  Explain you would like your listing removed from wink.com and mylife.com. You will be asked for your First Name, Last Name and Current State of residence.

  ii. Ensure the operator has all of your information removed by providing a former State lived in and/or one of your family members’ first names.
- Once they confirm removal, the listing will be off the site in 7-10 days.

BeenVerified, www.beenverified.com

- Scroll to the bottom of the homepage; click the PURPLE words “Remove my Info” under the “Help” title.

  Type in your first and last name, click “Search”.
- If you get receive “To Many Results”, refine your search in the yellow box to the left; click “Search”.

  Once you find your personal information, click the black arrow.

  Enter your generic email address and click “Send Verification Email”.
- Go to your generic email account and click the link provided in the email sent. You should see “Your Opt-Out Request is Confirmed”.

DOBSearch.com, www.dobsearch.com

- Locate your listing on the website, and check the box next it.
- At the bottom of the page, click “Manage my Listings”.

- Type “I AGREE” into the box.
- Find your listing again, and click “Continue”.
- Enter your email, and then go to your inbox and verify your account.

PeekYou, www.peekyou.com

- Go to www.peekyou.com, type in your information. If any your personal information is found – proceed.
- By clicking on your name, it will bring you to a profile. In that profile, next to your name, is a GREY link stating “Opt Out”.
- Fill out the PeekYou Opt-Out online form (remember to use your generic email address).
- Under “Actions” click “Remove my entire listing”. Then click the two boxes and “Submit”.

Whitepages, www.whitepages.com

- Search for yourself under “Find People”. If your personal information is found, click your name.
- Click the white “View Details” button.

  NOTE: If your results end with a blue button, your profile is only avaliable to premium members, and you will have to submitt a removal request through a support ticket at: https://support.whitepages.com/hc/en-us/requests/new
- Confirm that the profile is yours.
- If the profile is yours copy the URL/web address. If the profile is not yours go back to the previous page and try again.
- After you have found your profile page and have copied the URL/web address go to: https://www.whitepages.com/suppression_requests.
- Provide a reason for the removal request, when prompted to do so.
- Input your telephone number to verify the removal request.
- A four-digit code will then be provided. Soon after the code is provided you will recieve an authorization call at the number provided in the previous step. Follow the instructions and input the code when prompted.

Spokeo, www.spokeo.com

- Go to www.spokeo.com and search for your personal information. Click on all information that is yours. Copy the full URL of every page where your information is found.

- Scroll to the bottom of the page and click “Privacy”.
- Scroll to the bottom of this page, click BLUE words “Opt-Out”.
- On the “Removing Your Listing from Spokeo” page:

  Either paste or type URL where your information was found.

  Type in the generic email address you created.

  Click the button “Remove This Listing”.
- Go to your generic email account and click the link provided in the email sent. Clicking this link will complete the information removal (opt-out) process.
- You should see the words “This directory listing has been removed” in Spokeo.

  To verify this statement go back to www.spokeo.com and re-conduct a search for your personal information. Use other names. If additional information is found complete the previous steps again.

PrivateEye, www.privateeye.com

- Go to www.privateeye.com, scroll to the bottom of the homepage, click small BLUE words “Privacy Policy”.

  NOTE: Veromi, PeopleFinders, PublicRecordsNow, and PrivateEye are owned by the same parent company. Opting-Out on www.peoplefinders.com/manage/ will opt you out of all the sites.
- Scroll down to Section “7. How We Protect Your Personal Information”.

  At the bottom of that section, click “Click here to opt out”.

  Enter in your first and last name and state. Click “Opt Out”.

  Find your listing and click “This is me”. The click the BLUE button, “opt out my bio”, click the 3 buttons agreeing to the terms, and finally click “continue”.

Pipl, www.pipl.com (URL becomes https://pipl.com)

- You will need to the following steps with all of you name / information variances.
- Search for your personal information by typing in your First and Last Name as well as the City and State in which you live.
- If your information appears write down the main source of the information.
- Go to the main source of the information and change the privacy settings so it is not set to public. Now there is no clear cut way to get your information off of Pipl.

Archives, https://www.archives.com/optout

- Go to https://www.archives.com/optout and fill out the request form
- This will remove you from living person search results on Archives.
- Click “Submit” after filling out the form. Your information should be deleted after 2-3 weeks.

Instant People Finder, https://www.instantpeoplefinder.com/

- Enter your first and last name and hit “Find”.
- If you come up with a result, copy all the links to your profile.
- Go to https://www.instantpeoplefinder.com/optout.php and fill out the form.

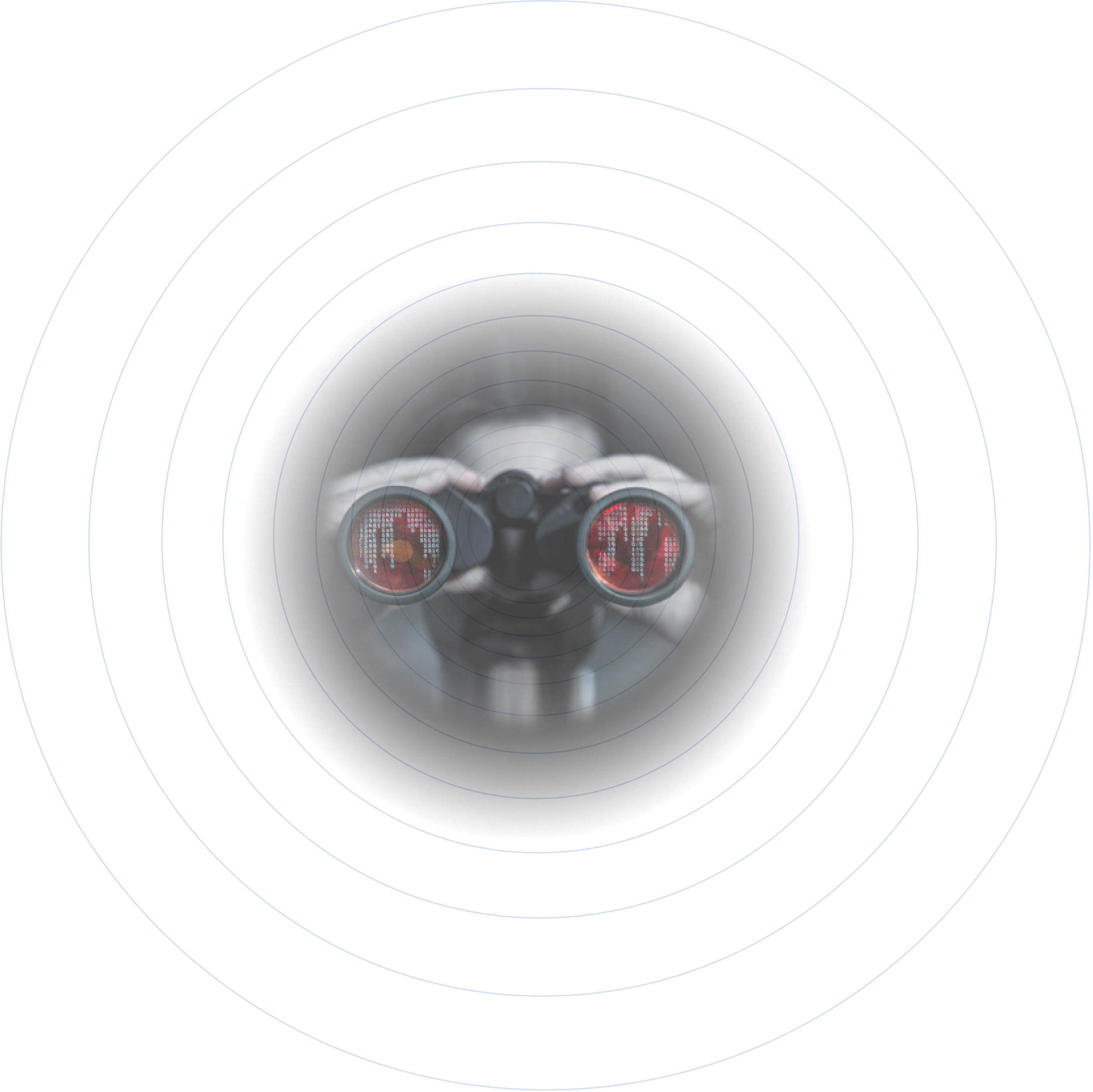
  Paste the URL in the appropriate box. If you have more than 1, put the older ones in “More”.

Store Reward or Loyalty Subscriptions

- Store reward or loyalty programs are the best way to save money and find out about the best deals. Hackers will target you either by sending you legitimate looking advertisements based on programs in which you are subscribed.
- Another way scammers will target you is luring you into signing up for loyalty reward programs based on your interests or past subscriptions.

Credit Monitoring Services

- There have been a number of data breaches and as such, it is important to monitor your credit in order to ensure it has not been compromised. There are a number of services that will monitor your credit report and credit score.
- Reputable credit monitoring services include Identity Guard, LifeLock, Experian, and TransUnion.



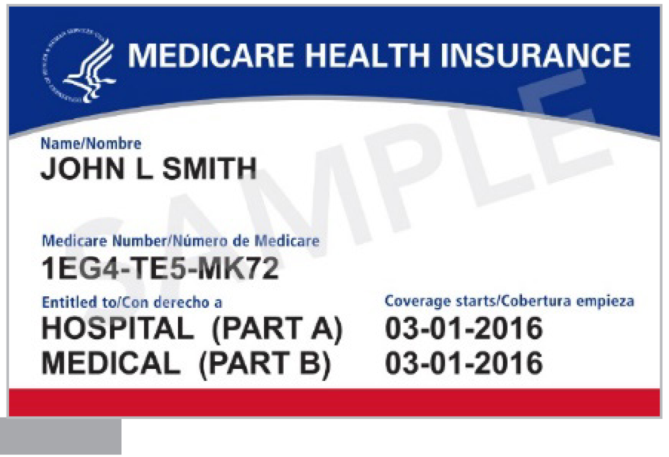
Protect Yourself: Medical ID Theft – Affordable Care Act

Research conducted by Ponemon Institute in 2013, and sponsored by the new Medical Identity Fraud Alliance, estimates that 1.84 million U.S. consumers at some point in time have been victims of medical ID fraud. This crime is increasing at an annual rate of 32% as of 2018. This makes it the fastest growing type of identity theft, according to the Identity Theft Resource Center.

Preventing Medical ID Theft

- Review bills closely. Medical bills and insurance statements may contain important signs that you are a victim of medical identity theft. Open and carefully review each medical document you receive, checking the itemized costs. If something looks suspicious, investigate by calling right away.
- Regularly check your medical and pharmaceutical records. Keep a list of the names and contacts for doctors, pharmacies and other health care providers you have visited in the past and refer back to this list in the event a problem arises. Obtain copies of your medical records from your doctors at least once a year and analyze them like you would a credit report. Look for treatments you didn't receive, fraudulent charges, etc. Check your pharmacy records and be sure all prescriptions are really yours.
- Check every medical insurance Explanation of Benefits (EOB). When your insurance provider sends an EOB, check the services charged against your own list of doctors visited, treatments received and dates of service.
- Know your rights under Health Insurance Portability and Accountability Act (HIPAA). If you think you're a victim, you should obtain a copy of the HIPAA, to learn your rights under the law. Every hospital and insurer must publish a copy of practices and privacy rules in compliance with HIPAA and must make them available upon request. If you see a HIPAA violation in a medical setting, ask about it.
- Ask your health care provider if they have a privacy policy and how it's enforced. Find out if that policy applies to their vendors, such as third-party billing companies. Does your dentist keep your records in a locked cabinet? Does your doctor use a crosscut shredder? Was your ID checked when you signed in? Smaller health care providers may not be aware of things they can do beyond HIPAA regulations.
- Check your medical records regularly. The process of requesting and obtaining your medical records can be time-consuming and expensive, but it can reveal serious medical fraud issues. At a minimum, keep a list of the names and contacts for doctors and other health care providers you have visited in the past and refer back to this list in the event of an issue.

- Do not allow others to use your medical ID. This includes uninsured family members or friends. About 30 percent of medical ID theft victims shared their medical ID with the person who used the credentials. Another 28 percent of victims say a family member took their medical ID without permission.
- Don't provide your SSN without reason. Many medical practices ask for SSNs even though they aren't necessarily needed. If you're asked for your Social Security number, ask why. Don't provide it unless it is absolutely needed.
- Don't just toss old records. When disposing of old medical records, explanation of benefits forms, etc., dispose of them properly. Always shred or destroy records you're tossing out and keep any records you need in a secure place.



MEDICARE HEALTH INSURANCE

SAMPLE

Name/Nombre
JOHN L SMITH

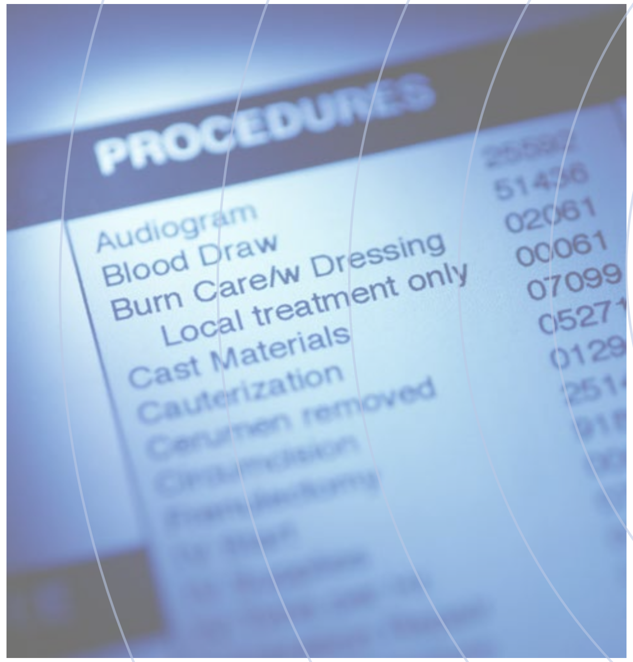
Medicare Number/Número de Medicare
1EG4-TE5-MK72

Entitled to/Con derecho a	Coverage starts/Cobertura empieza
HOSPITAL (PART A)	03-01-2016
MEDICAL (PART B)	03-01-2016

Six Predominant Threats Used for Medical Identity Theft

- **Phishing:** Phishing email messages, websites, and phone calls are designed to steal money. In these attacks, criminals will spoof an email address pretending to be from a legitimate organization in an attempt to get users to click on a malicious link or unknowingly submit confidential data. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer. Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website. One of the most popular scams is getting a user to avoid a negative consequence and could include emails with subject lines such as "if you don't sign up for a new health care plan you'll get fined" or "you need to comply with this new law."

  Reference Section 6: Social Engineering for more information about Phishing attacks.
- **Insurance Card Scam**: The Better Business Bureau has issued a warning that con artists are trying to lure people into providing Social Security numbers or bank account information so they can "send a new insurance card." With that information, the fraudsters can steal your identity. Remember, unlike Medicare, there is no such thing as an ACA insurance card.
- **Impostors Posing as Advisers:** The Affordable Care Act created a designated breed of advisers known as "navigators," who generally work at nonprofits like the United Way or local agencies. Navigators are supposed to help answer questions and to help individuals enroll for coverage. Imposters are now calling and emailing unsuspecting consumers, posing as navigators and trying to steal their identities or sell them phony health insurance. The real "navigators" should never ask you for personal information, and you should never give it out. Remember that no one from the government will call you, email you or show up to your house regarding the Affordable Care Act.
- **Employee Insurance Scams:** Reports of employees being targeted in spear phishing campaigns is alarming. Many employers will, in fact, contact their employees due to changes in existing insurance. Any emails coming in that look legitimate should not be clicked on until you have an additional confirmation via telephone or an email address in your contacts.
- **Medicare Scams:** Medicare related scams continue to exist with scammers using a variety of means to steal information from a vulnerable population. Scammers use any number of phishing and other social engineering methods to obtain exploitable PII and account information. Additionally, the newly issued Medicare cards include a new substitute ID number unaffiliated with your social security number. The issue that has arisen is the number is almost as sensitive as a social security number in relation to Medicare fraud. Remember, Medicare will only contact you through paper mail, never through e-mail, phone, or text.
- **Spoofed Websites:** Health care.gov is the official website for the ACA. Any other site suggesting it is the site or an alternative is a scam. Even if you receive an email naming health care.gov as a hotlink, it's a scam. Phishers can easily spoof a web address in an email.



Protect Yourself: Old Devices & Tech Gadgets

In 2017, a tech research company, Gartner, estimated 1.5 billion cell phones were bought. Most mobile devices hold sensitive information like addresses and phone numbers, passwords, account numbers, email, voicemail, and text message logs. Because devices are always updating, people want the newest technology and are turning in their old devices for new ones. Therefore, when getting rid of your old device(s), it's important to take steps to help ensure this information doesn't fall into the wrong hands.

Back Up Data

First things first, you should back up your entire system, before wiping the device and getting rid of it. If something goes wrong or you change your mind about selling your device, you will still have all your files available. Additionally, you will be able to put the files on your new device.

The best option to back up your system is to copy your files to external storage. You will need to find an external storage device big enough to hold all your files. To back up your operating system, open Control Panel > System and Security > Backup and Restore. On the left side, choose the option Create a system image and then under "Where do you want to save the backup?" select "On a hard disk". The drop down menu will allow you to choose your external storage. Then click Start backup.

- Backing up a Mac system has a few more steps. First, the best way to expedite this process is to use an external hard drive that has no other data on it. You will most likely have to reformat the hard drive before storing anything on it.

  Connect your external storage to your Mac

  Launch Disk Utility. This is usually located in Applications under the subheading Utilities. Find the hard drive you want to reformat.

  In the Disk Utility window, choose Erase. Then rename your hard drive. In the Format menu, choose "OS X Extended (Journaled)". In the Scheme menu, if you want to use the drive on a Mac

  Go to System Preferences > Time Machine > Use as Backup Disk. Your back up will begin automatically.

- If you wish to back up your mobile device, go to Settings > Backup and reset > Backup my data > Automatic restore.

Another method of backing up your files is through third party software or apps. While these may be more convenient, having a physical external storage is safer because as long as it is not connected to a device or Internet, it cannot be hacked.

Check for Removable Media

After you have backed up your content, check your device for any removable storage. For computers, that means checking the DVD drive, card reader, and USB ports for old or forgotten media.

In addition to internal storage, phones and tablets often have a tiny removable microSD memory card, which houses photos, media files, and sometimes app data. The card is likely hiding beneath the back battery cover, near the SIM card slot, or even behind the battery. You'll want to remove it and, if your phone has one, the SIM card, since it contains your phone number and probably at least some of your contacts.

- The product manual will inform you if you have a microSD card, and if so, where it is located.
- Do NOT encrypt the SD card if you plan on using the data stored on it in the future on a different device. When you encrypt the data, it can only be accessed from the originating device. When you get rid of an old device, decrypt the card before the factory reset. It can then be put into another device.

For digital cameras or media players, removing the memory card is the obvious step. But remember many devices, particularly older digital cameras, have some internal storage as well. So connect the device to your computer via USB and delete or remove internal-memory files.

Personal Computers

To make sure your personal data isn't recoverable by reasonable means, do a secure wipe. This not only deletes your data but also overwrites the data a certain number of times, which makes the data more difficult to retrieve. There are several safe and user-friendly software data eraser tools available, such as BitRaser for File, SDelete, Eraser, and DBAN.

- Out of all of these options, the best one is BitRaser for File. It will not only erase the files on your computer, it will also erase all your Internet activities, such as cookies and passwords to websites. Another unique feature is it will erase Solid State Drives (SSDs), which most erasure software fails to target.
- You can also securely erase a Mac or PC for free by burning DBAN to a CD, DVD or flash drive and run it from there. When you boot your computer with DBAN, you can choose various levels of secure erasing and select which drives you want to erase, if the computer has more than one. Or you can type "autonuke" to securely erase all drives.

  DBAN is a good choice as long as you don't want to repurpose the PC with the OS intact. If you're using an older version of windows, you may be able to do a factory reset with Windows reinstalled, with an option to do a secure erase in the process.

- Secure erasing can take several hours or even days to complete, depending on the size of your drives.

- You can also use this method to erase external portable hard drives securely. Just take care to erase the correct drive and not a drive with data or an operating system you want to keep.

Smart Phones and Tablets

The easiest way to securely erase a smart phone or tablet is to encrypt the device, then do a factory reset. First, though, remember to back up any files you want to keep and remove the microSD and SIM cards.

iOS

- For the Apple devices, data should automatically be encrypted if you have a passcode (screen lock) enabled. The passcode is used to generate an encryption key, and when you factory-reset your phone, the passcode and encryption key are securely deleted. Any data that's left behind is securely scrambled, and thereby inaccessible to all but the highest-level data-recovery experts.
- If you haven't already set a passcode in iOS, you can do so by tapping Settings > Passcode or Touch ID and Passcode.

  Also check on this screen to make sure that data protection is enabled; if it isn't, toggle it on.
- Backup your data. If you have an Apple Watch, unpair it from the old phone. Next, backup files using iCloud. If you use iCloud, note that you only get 5GB of storage for free. For iCloud backup go to Settings > [your name] > iCloud > iCloud Backup.

  NOTE: Sign out of iCloud before you erase your device. If you do delete information while signed into your accounts it will delete your content from the iCloud servers and any of your devices signed into iCloud.
- Erase your content. Go to Settings > General > Reset > Erase All Content and Settings. Tap Erase.

Android

- Remove the Factory Reset Protection. This tool was introduced in order to prevent thieves from being able to steal your phone, wipe it, and then use or sell it. This step will differ slightly depending on the type of Android you own.

  Go to Settings and find the Screen Lock (or some variation) tab. Change it to None.

  Then, go to Settings > Accounts (or some variation). Go to the account(s) and find the option to remove the account. If you have a Samsung, go to Settings > Lock screen and security > Find My Mobile. Enter your password, tap your account at the top, and select More > Remove account.
- Encrypt your data. Again the exact method will vary depending on the type of phone. First, as mentioned above, if you want to use the SD card and/or SIM card in another device, remove it before encrypting the data you plan on wiping.

  Go to Settings > Security > Encrypt phone. If your phone is a Samsung Galaxy, go to Settings > Lock screen & security > Protect encrypted data.
- Factory reset your phone. Once again, the steps may differ from phone to phone.

  Go to Settings > Backup & reset > Factory data reset, then tap Reset phone/device. On the Samsung Galaxy, go to Settings > General Management > Reset > Factory data reset, then tap Reset device.
- An optional step, if you want to be absolutely certain all your data has been erased, you can go to the app store and download iShredder 6.

Gaming Consoles

There's no easy way to do a secure wipe of game-console storage, so you'll have to rely on the standard factory reset. You can physically remove the hard drive and hook it up to a PC or Mac, and securely erase it. But generally, the sensitive data on consoles is stored in non-removable Flash memory.

As we noted earlier, you'll want to remove any media cards and either keep them, or securely erase those as well before placing them back in the system. You can securely erase standard SD cards with a free app from the SD Association. After installing and starting the SD formatting program, choose the card's drive letter on your system, then click the Format button on the bottom.

Then from the resulting menu, choose "Format Type: Full (OverWrite)". Again, this will take quite a bit of time, depending on the SD card's capacity and write speed.

Xbox One

- Back up your content. Purchase a compatible hard drive that uses USB 3.0 and has at least 256GB of storage. Additionally, don't use a hard drive you used for your PC or Mac otherwise everything will be deleted.
- Connect the hard drive, then press the Xbox logo on your controller to open up the guide.
- Go to Settings > System > Storage > Manage Storage. Select all the games or apps you want to transfer in the menu and begin the transfer.
- Delete your Xbox Live account. This is important! If you don't do this, people will have direct access to you credit cards if you directly purchased from the console.
- Reset your console. Press the Xbox logo on your controller. Go to Settings > System > Console Info > Reset Console.

Nintendo Wii

- Before resetting your Wii, first delete the Wii Shop Channel, which stores your account and purchased games. To do this, select Wii Shop Channel from the main menu, the Start > Settings > Remove Wii Shop Channel Account > Remove
- Once that's done, reset the Wii to factory settings by clicking the "Wii" button from the main screen, then selecting Wii Settings. Click the arrow on the right twice to get to the third settings page. Then select Format Wii System Memory, then Format.

- If you have parental controls enabled, you'll have to enter your PIN. Then select Format, and your Wii will begin the factory-reset process.

Sony PlayStation 4

- Back up your data. Choose an appropriate external hard drive to store your content. You might need to do some research to choose the best hard drive. Plug in the hard drive. In order to format the hard drive go to Settings > Devices > USB Storage Devices and select your hard drive. Then select Format as Extended Storage and OK. To begin the transfer by going to Settings > System > Back Up PS4.
- Deactivate as primary PS4. Make sure your account is no longer linked to the system you intend to sell by going to Settings > Account Management > Activate as Your Primary PS4, then select Deactivate.
- Initialize your PS4 in order to wipe all your data off the console. This might take a few hours. Go to Settings > Initialization > Initialize PS4 > Full.

4. Nintendo 3DS Handheld Consoles

- To remove all of your personal data from these gaming gadgets, go to the "System Settings" icon on the lower touch screen (the icon with the wrench symbol). Within the "System Settings" menu, select "Other Settings", and then scroll over to the fourth menu page and select "Format System Memory".
- At this point the system will prompt you to delete your Nintendo eShop account. The eShop is Nintendo's equivalent of iTunes, but it is tied to your device, and this is where your credit-card and purchase information is stored, so you'll want to make sure to delete the account.
- Just open the Nintendo eShop and select "Menu". Select "Delete Account" and then "Confirm".

- Formatting the 3DS will not wipe anything you have stored on the removable SD card, so remove it.

Properly Get Rid of Your Device

A report conducted by the United Nations, reported 44.7 million tons of "e-waste" was discarded in 2016, and of that waste, only 20 percent was disposed properly. Whatever method you choose to dispose of your electronics, make sure you also properly clean the data off the device.

- Look up recyclers. Most likely your county will have a facility to recycle electronics. Also, many tech companies, such as Best Buy and Dell will recycle electronics.

Donate your device. There are nonprofits and charities that will take your old electronics. Many of these electronics go to seniors or underprivileged, sometimes in less developed countries. Some of these charities include Dell Reconnect, AmericanCellPhoneDrive.org, World Computer Exchange, and eBay for charity.

- If you do decide to donate, get a receipt of your donation, and you can claim it as a deduction on your taxes.

Trade-in your device. Many companies will accept trade-ins. In some instances, you can receive a gift card in lieu of a new device. Check the company's policies to understand how their trade-in process works.

Sell your device. There are many platforms in which to sell your device, some of which are Facebook Marketplace and Craigslist. Again, if you choose this method, along with all the methods above, make sure you wipe all the data.

Bottom Line

Even if you follow the above suggestions to securely delete files from electronic devices, the only foolproof way to make sure no one can retrieve your data is to physically destroy hard drives and memory chips (following proper safety precautions).

CyberHOUND says ...

We'll help you sniff out the bad guys! Stay Safe Online!

Pentagon Force Protection Agency
Threat Intelligence Center

703-693-5000

pfpa.pentagon.iid.mbx.tmdd@mail.mil
https://extranet.pfpa.mil/