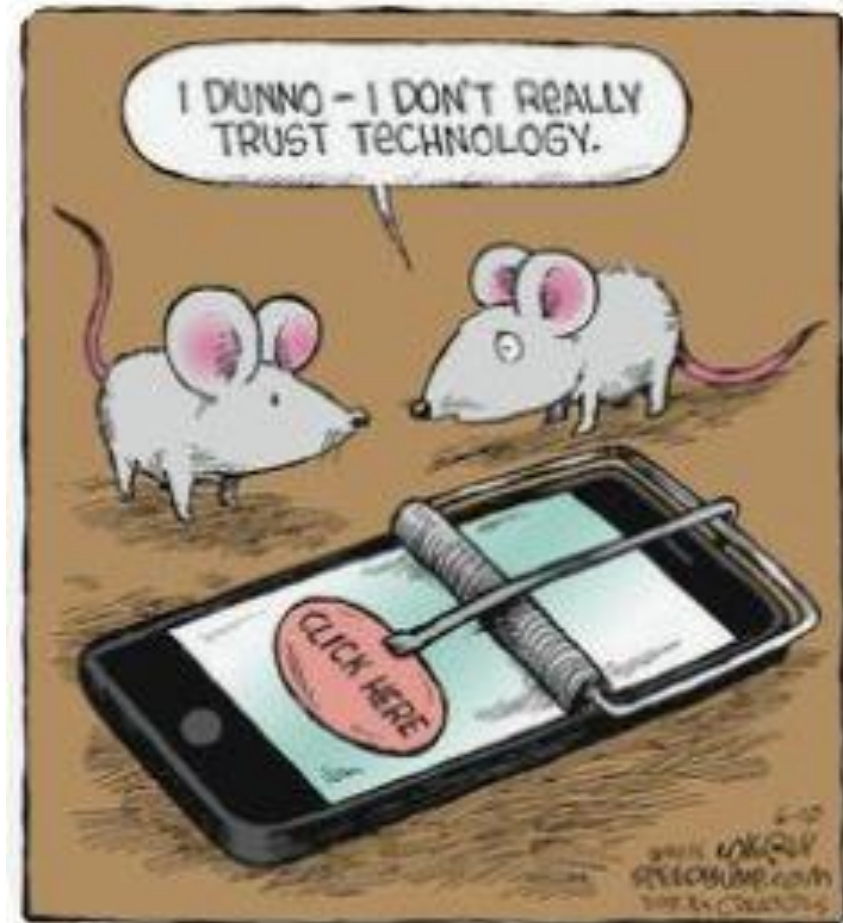
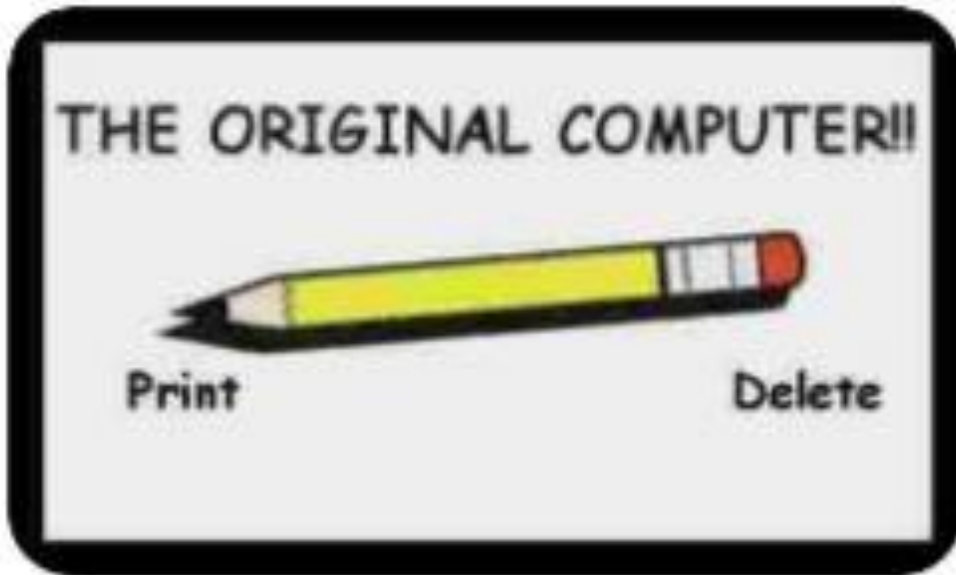




---

# CYBERSECURITY

PROTECTING YOURSELF IN TODAY'S WORLD



**Technology dominates today's world and can be overwhelming. However, knowledge is power and learning about cybersecurity can protect your data from theft and damage.**

# IMPACT OF CYBERCRIME

- According to FBI data compiled by CCTV Camera World, victims lost a record \$4.2 billion to cybercriminals in 2020, up from \$3.5 billion the year prior.
- Utahns were near the top of the list, with the average victim losing \$9,562 making Utah the nation's fifth-highest in cybercrime losses.
- The same report shows the total cost of cybercrime incidents reported to the FBI has gone up by nearly 800% since 2011, from \$485.3 million to \$4.2 billion
  - The best advice: **Never click on links in text messages or emails from people you don't know; never assume a person calling you is who they say they are.**

---

## 1. **There is a hacker attack every 39 seconds.** *(Source: Security magazine)*

By the time the average person takes a selfie and uploads it to Instagram, the next hacker attack has already taken place.

## 2. **Cybercrime is more profitable than the global illegal drug trade.** *(Source: Cybersecurity Ventures)*

The profit from the illegal drug industry amounts to around \$400 billion annually. For comparison, cybercriminals have earned a total of around **\$600 billion** in 2018.

## 3. **Hackers steal 75 records every second.**

Cybersecurity facts show us the average number of records stolen per second. Breaches are actually much rarer than that – it's just that each breach allows for a lot of records to be stolen.

## 4. **66% of businesses attacked by hackers weren't confident they could recover.**

75% of all businesses don't even have a formal cyber attack response plan.

---

**5. 80% of hackers** say humans are the most responsible for security breaches. *(Source: Thycotic.com)*

**6. The cybersecurity budget in the US was \$14.98 billion in 2019.**

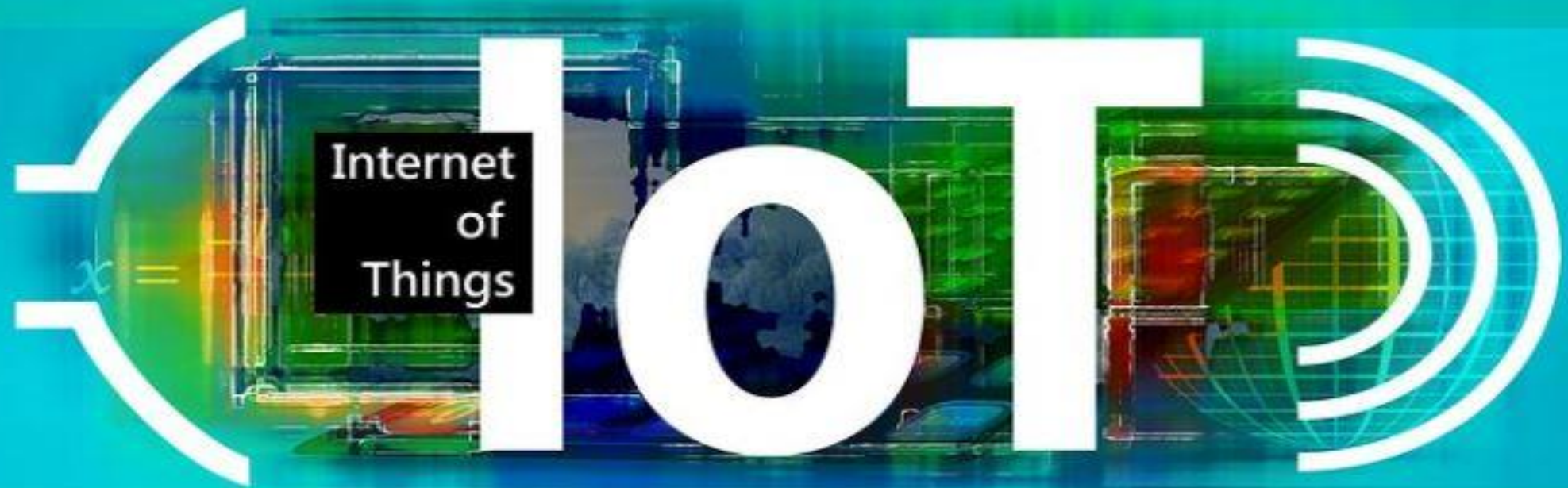
**7. White hat hackers (“good” hackers who test systems looking for weak spots) earned over \$19 million in bounties in 2018.**

**8. There are over 715,000 cybersecurity experts employed in the US alone.**

**9. Russian hackers can infiltrate a computer network in 18 minutes. North Korean hackers need just under 2 ½ hours; Chinese hackers take longer – about 4 hours.** *(Source: Crowdstrike)*

**10. 68% of black hat hackers (“criminal” hackers) say multi-factor authentication and encryption are the biggest hacker obstacles.** *(Source: Thycotic)*









*"Bad news - the scale is threatening to cut off  
our access to the fridge..."*





# CYBER ATTACKS



DoS



Hacking



Ransomware



Phishing



Spoofing



Malware



Spamming

TYPES OF CYBER ATTACKS

## Impersonation

One of the greatest dangers that the internet creates is the ease with which mischievous parties can impersonate others. These can be accomplished with a website or with emails.

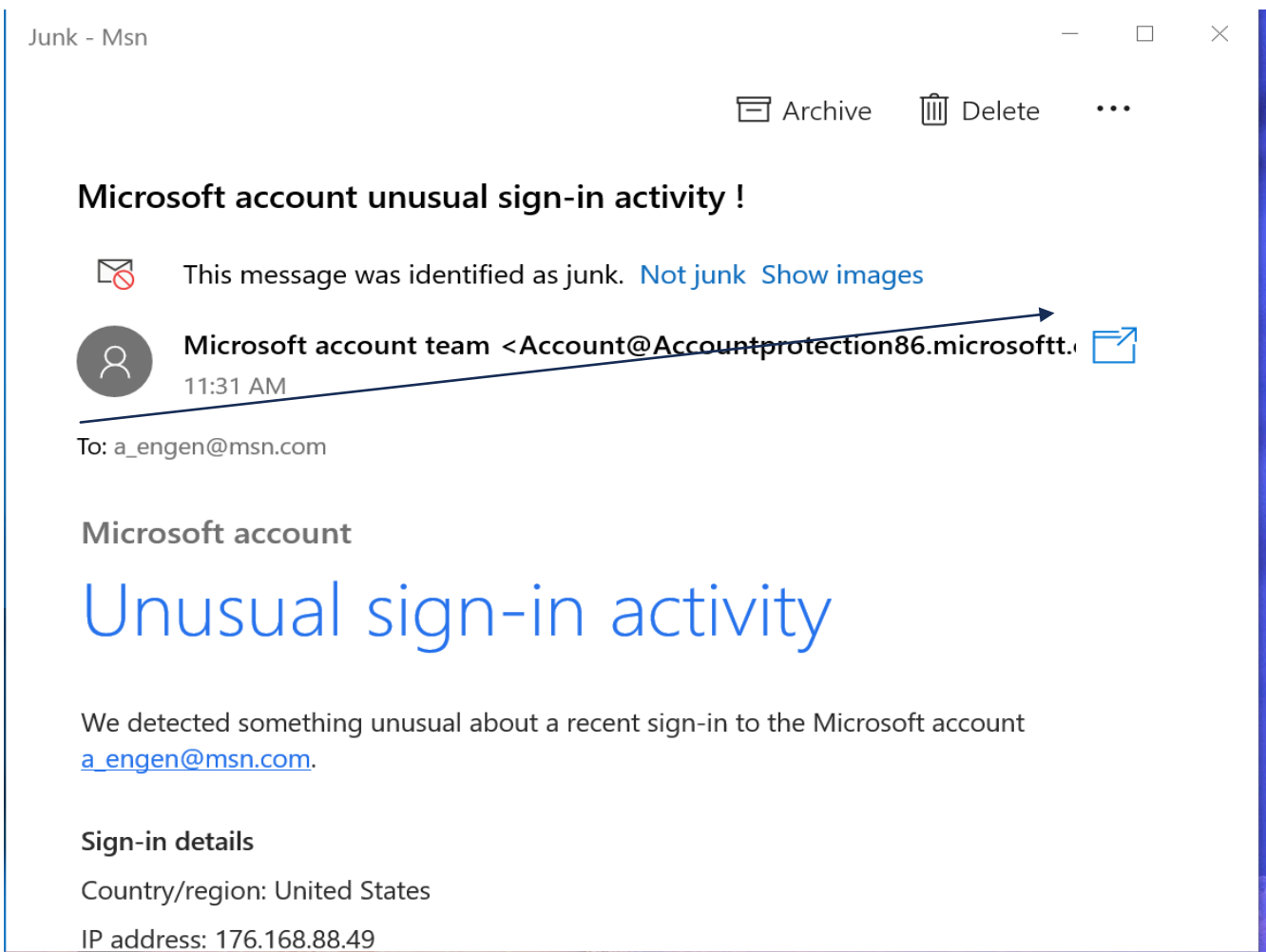
## Phishing

An attempt to convince a person to take some action by impersonating a trustworthy party that reasonably may legitimately ask the user to take such action. Most of these emails contain fraudulent links that could result in a monetary loss or expose your personal address book.

Email Phishing scams use spam, fake websites constructed to look identical to real sites, email and instant messaging to trick you into divulging sensitive information like bank account passwords and credit card numbers. Once you take the phisher's bait, they can use the information to create fake accounts in your name, ruin your credit and steal your money or even your identity.



## Example:



Email is the primary source of malware distribution with 95% of malware being delivered via email.

This email looks creditable but check out the actual sender's email. The object of this example is to get access to your Microsoft account information. If you clicked the link, you would be taken to a site that would collect your account information. The hacker would then have access to all your secure and authentication information.

Phishing scams include blank emails that lack content. Once the email is delivered, the scammers know your account is active and a second message follows that tries to engage you in a conversation. Best to set up a "rule" in your email program to send all emails from the source to your junk folder.

## CYBERSECURITY

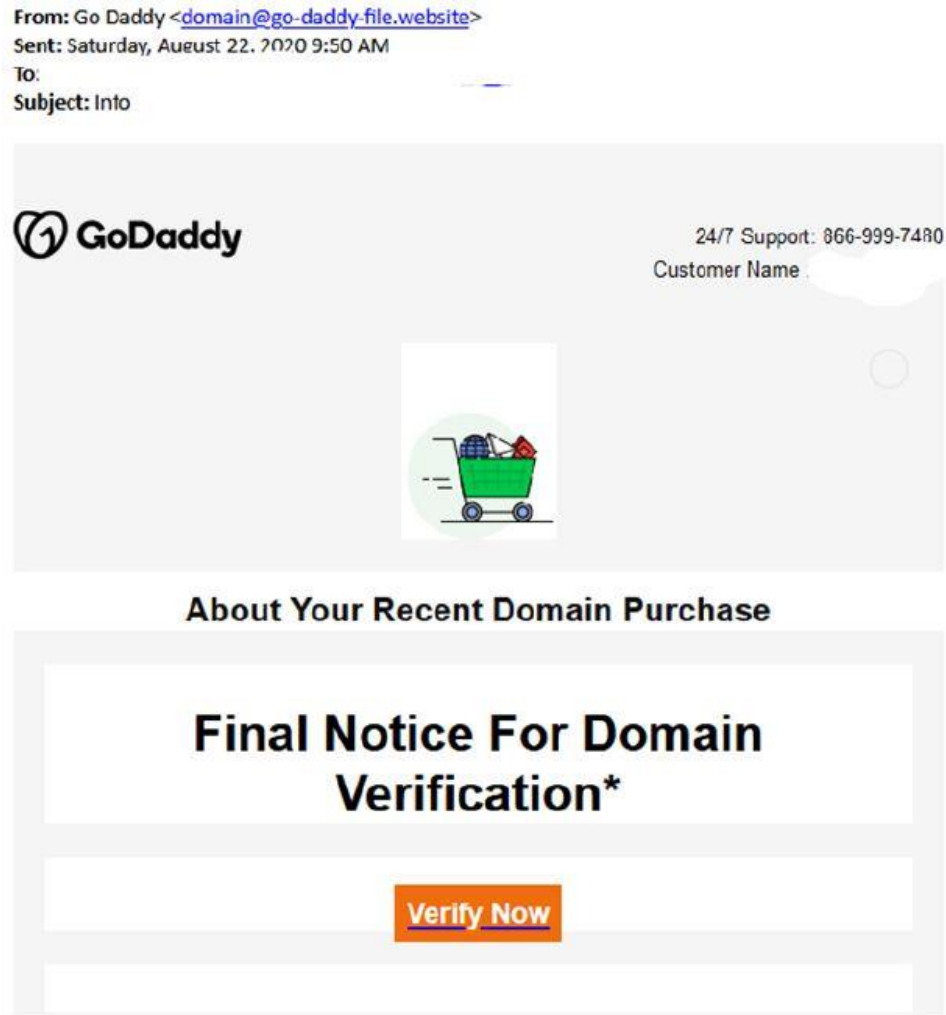
### Infographic - Phishing Flow Diagram Using PayPal Example





**Spear Phishing:** Similar to Phishing, these attacks target a specific person, business, or organization. Their goal is to get credentials that give them greater access to the recipients' accounts.

Example:



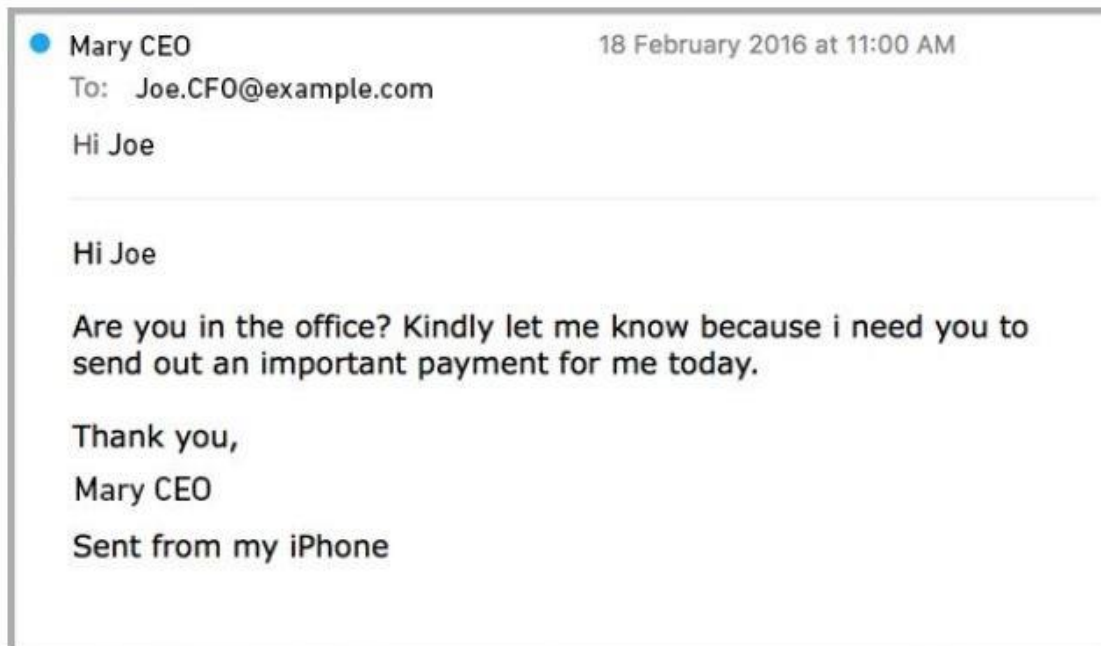
The sender of this email could gain greater access to your personal or company credentials if you clicked the “Verify Now.”

Best to go to the online login site of your email provider and check the notifications or, if possible, call the provider's tech support to see if the company sent the original message.

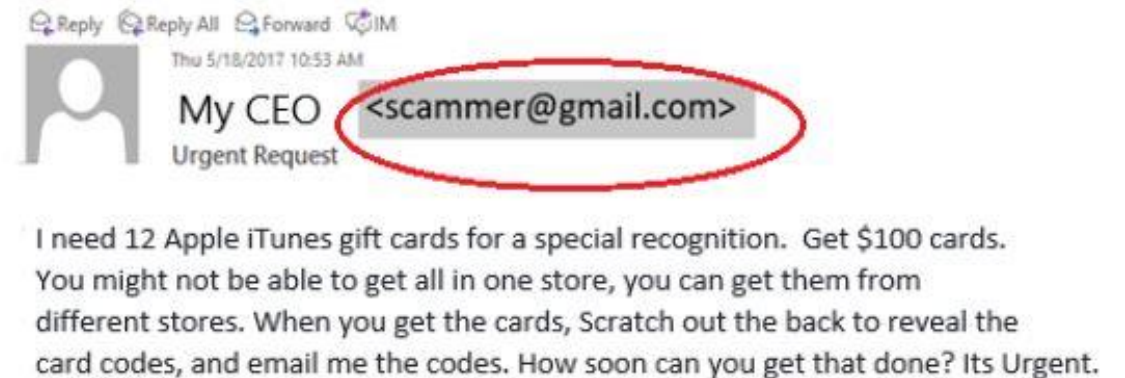
Recently, emails from phony title companies ask recipients to verify the attached documents and, from there, get more information about your mortgage, bank and other accounts.

**CEO/Friend Fraud:** Similar to Spear Phishing, these emails impersonate the CEO, senior executives or close friends. These attacks often ask recipients to take specific actions that will directly net the sender significant returns and make the recipients appear incompetent. Purchasing gift cards and sending the card number and PIN to the sender fall into this category.

Examples:



If responded to, a second email would provide a bogus link for the payment to be completed, netting the criminal whatever funds transferred.



Always check the email beside the display name. If the two do not match, do not respond, and never purchase gift cards! Call the person who it appears sent the message to see if they are the legitimate sender.

**Smishing:** Phishing attacks that come via text messages, known as SMS.

Example:

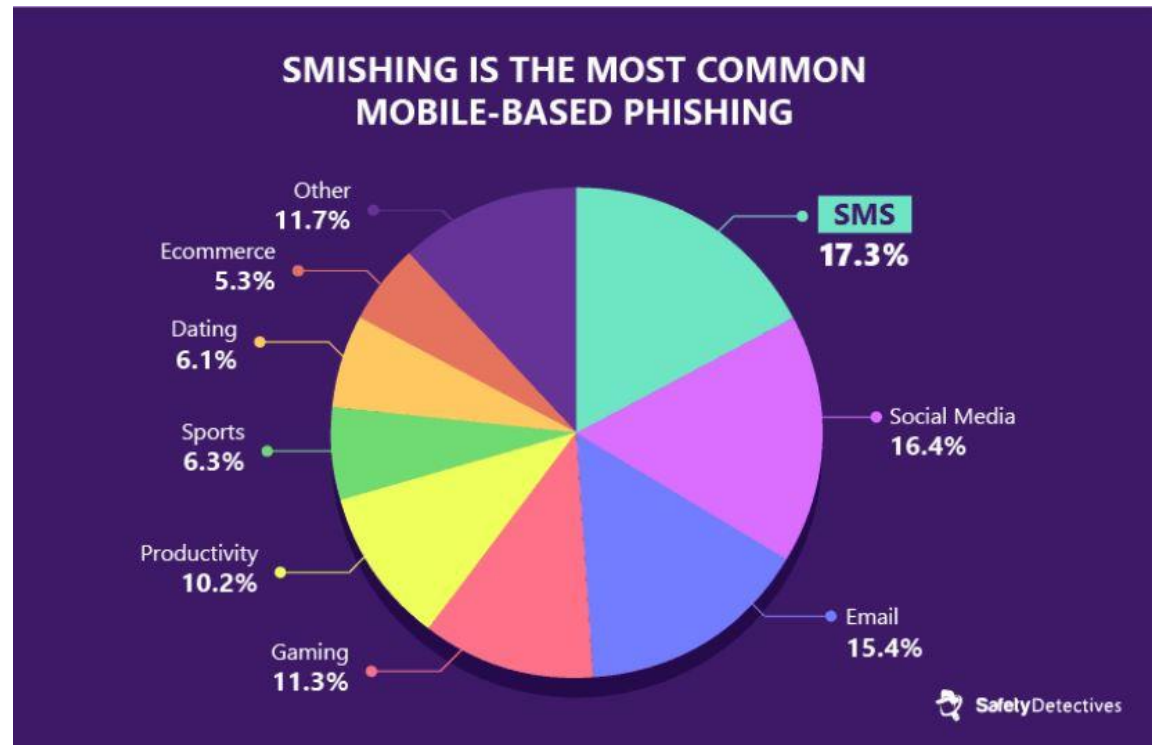


If you don't know the sender, call the customer service number on your credit card or account and verify. Also, check your email as most legitimate companies who are checking on your credit card and account information will also send you an email. It's time consuming but always best to go to the company directly and check your account by logging onto the company's website.

## Smishing attacks can steal user information using fake two-factor authentication (2FA) messages.

If you've ever received a one-time password to verify your identity on PayPal or Amazon, then you've used SMS (text)-based 2FA — however, this very same technology can be used to steal your login information, redirect you to fake login pages, or even use hacking techniques to send one-time passwords intended for your phone to completely different devices.

That's one big reason why the National Institute for Standards and Technology (NIST) recommends against using SMS-based 2FA passwords — if you don't rely on it, you won't fall victim to it. SIM swap fraud is increasing dramatically.





## SIM SWAP FRAUD:

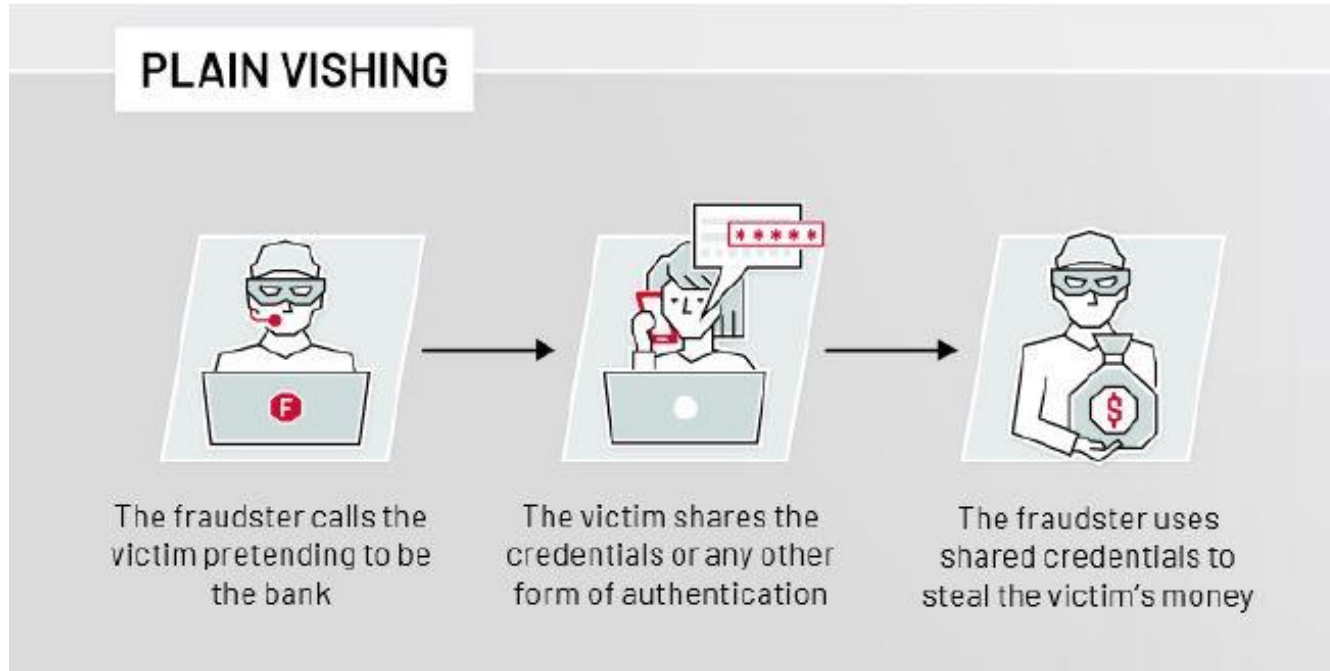
This occurs when a hacker convinces your cell phone carrier they are you and gets the carrier to switch your phone number to a different SIM - one that they own. ... It doesn't require a hacker to have any technical knowledge, just a SIM card and a phone call to your provider. SIM swaps also occur when phone company employees are bribed to deactivate your SIM card and switch the info to the hacker's card.

- Hacker intercepts your calls and texts, including all account 2FAs.
- First clue is your phone loses service
  - If that happens, block all financial accounts; set new PIN immediately
  - Call cell phone company and cancel account and phone number
  - These steps need to be done immediately as hackers work fast to wipe out your bank accounts.

To prevent SIM swap,

- Do not use text or phone call 2FA. Instead, **use email or a password protected authenticator app such as Google Authenticator, Microsoft Authenticator or Authy.** All are free and have different features so research the one that is right for you.
- Do not give out personal information on social media. Use fake birthdate and other false information on sites that don't require legal personal information. (Hackers often need personal info to convince phone company employees they are you.)
- Never rely on one single form of authentication.

**Vishing:** Voice-based phishing using plain, old telephone service.



Use caller ID or ask for a number to call back for verification. Or, look up the phone number of the company and call. Legitimate businesses do not require you to provide account credentials or credit card numbers over the phone.

## Interception Attacks


These attacks occur when hackers capture information in transit between computers. If the data is not properly encrypted, the attacks may misuse it.

Many cyber interceptions involve stealing the victim's data. People, businesses, nonprofits, and governments are all vulnerable. The attackers are looking for things they can monetize, such as:

- Identity information
- Compromising photos or health data for blackmail schemes
- Information that can be erased and held for ransom
- Password lists to breach other systems
- Confidential work info that gives the attacker a competitive advantage
- Travel plans so attackers know when homes are available to be burglarized

These attacks fall under the heading of **Malware** or **Malicious Software** which is an all encompassing term for software that intentionally inflicts damage on its users who typically have no idea that they are running it. **Always ask companies to send and receive only encrypted personal information.**

Malware comes in several varieties:



**Viruses:** Viruses replicate themselves by inserting their own code into computer systems. They are usually introduced in a data file, such as a Word document. They can significantly impact the performance of the host computers, or they can be hardly noticeable.

Viruses are designed to spread from device to device. These self-copying threats are usually designed to damage a device or steal data. Think of a biological virus – the kind that makes you sick. It's persistently nasty, keeps you from functioning normally, and often requires something powerful to get rid of it. A computer virus is very similar. Designed to replicate relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

Some computer viruses are programmed to harm your computer by damaging programs, deleting files, or reformatting the hard drive. Others simply replicate themselves or flood a network with traffic, making it impossible to perform any internet activity. Even less harmful computer viruses can significantly disrupt your system's performance, sapping computer memory and causing frequent computer crashes.

Even if you're careful, you can pick up computer viruses through normal Web activities like:

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening spam email that includes images or scripting or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements



**Worms:** These are standalone pieces of malware that replicate themselves without the need for hosts to spread. They often propagate over connections by exploiting security vulnerabilities or target computers. They consume bandwidth and often slow down network connections.


One of the most notorious worms was the ILOVEYOU worm sent in May 2000. It was transmitted via email with an attachment labeled Love-Letter-For-You. The attachment contained the worm which started overwriting random files on the user's PC. It then sent copies of itself to everyone in the user's address book. It infected over 10 million PCs and caused the Pentagon, the British government, and the CIA to completely shut down their mail systems. Over 45 million computers were infected by this malware.

**Trojans:** Appropriately named for the historical Trojan horse, this malware is either disguised as non-malicious software or hidden within a legitimate, non-malicious application or digital file.

Trojans are often spread by some form of social engineering – tricking people to click on a link, install an app, or open an email attachment.

Unlike viruses and worms, they do not self-propagate but depend on the user to take an action to send them along.






**Ransomware:** This type of malware demands that a ransom be paid to some criminal in exchange for their infected files to not suffer harm.

The malware often encrypts user files and threatens to delete the encryption key if payment is not received. Ransomware is most often delivered to victims as a Trojan or a virus.

The rise of ransomware over the past few years is an ever-growing problem that has quickly become an extremely lucrative criminal enterprise. Targeted organizations often believe that paying the ransom is the most cost-effective way to get their data back — and, unfortunately, this may also be the reality.

The problem is that every single business that pays to recover their files is directly funding the development of the next generation of this cyber threat. As a result, it continues to evolve, with more sophisticated variants and more specific targeted cyberattacks. The costs continue to rise as well.

Recent research from Cybersecurity Ventures predicts that these attacks will cost the global economy \$6 trillion annually in 2021!



**Scareware:** This type is just what its name implies; it tries to scare people into taking some action and is often linked to the need to upgrade a computer security feature. A message appears on the device that says it has been affected by a virus that only a particular software can remove, and a link is provided to a bogus site that captures the user's information.

**Spyware:** Software that surreptitiously and without permission collects information from a device. It may collect keystrokes, which are useful for capturing passwords, video, audio, or screen images.

- While it may be a tough pill to swallow, fully reading terms and conditions and privacy statements before installing software or using a website helps users understand how their use will be tracked
- Never click on ads from unfamiliar or illicit-seeming sources and beware of false buttons that appear they will close a pop-up.
- Use an up-to-date web browser designed to protect against spyware

**Adware:** Software that generates revenue for the party operating it by displaying advertisements on a device. It is malware when it is installed and runs without the owner's permission.

**Denial of Service Attacks:** These attacks cause an interruption in an authorized user's access to a computer network, typically one caused with malicious intent.

---

**Botnets:** Botnets have been one of the most common methods of malware deployment for the past decade, infecting hundreds of millions of computers.

As botnets infect new technologies, such as Internet of Things (IoT) devices in homes, public spaces, and secure areas, compromised systems can put even more unsuspecting users at risk. Most botnets have an extremely small footprint, meaning they bog down your system or use a lot of system resources, so it can be difficult to recognize when your machine is being used by a criminal for malicious purposes.

**Zombies:** A **zombie** is a computer connected to the internet that has been compromised by a hacker via a computer virus, computer worm, or Trojan horse program and can be used to perform malicious tasks under the remote direction of the hacker. Zombie computers often coordinate together in a botnet controlled by the hacker and are used for activities such as spreading email spam and launching distributed denial-of-service attacks (DDoS attacks) against web servers. Most victims are unaware their computers have become zombies.

**Data Destruction Attacks:** Attacks that permanently damage or destroy the data. They are often used if someone refuses to pay a ransomware ransom.

Adapted from:

*National Assistance League Connections 2021*: Cheri Kassinger

*Cybersecurity for Dummies* by Joseph Steinberg

*Cisco Umbrella*, <https://umbrella.cisco.com/ransomware>

*What is a Cyberattack?*, <https://www.ibm.com/services/business-continuity/cyber-attack>

*Savvy Security: Ten Phishing Email Examples You Need to See*,

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>



## Public Wi-Fi Isn't Secure

When you're using your favorite coffee shop's Wi-Fi, there is no guarantee the website is secure. If the network isn't secure, and you log into an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and send. They could hijack your session and log in as you. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

A scammer also could use your account to impersonate you and scam people on your contact list or test your usernames and passwords on other websites — including sites that store your financial information. If a scammer gets your personal or financial information, they could steal your identity.

When you sign on to public Wi-Fi, you may also be sharing your data with the companies providing the Wi-Fi. Many public Wi-Fi networks such as in airports and hotels will also prompt you to install a “digital certificate” to use their internet. They may do this to scan your traffic for malware — but this also allows them to read your traffic, even if it's to a site using https (which encrypts information).

But there are steps you can take to protect your information, even in public.

## Ways To Protect Your Information

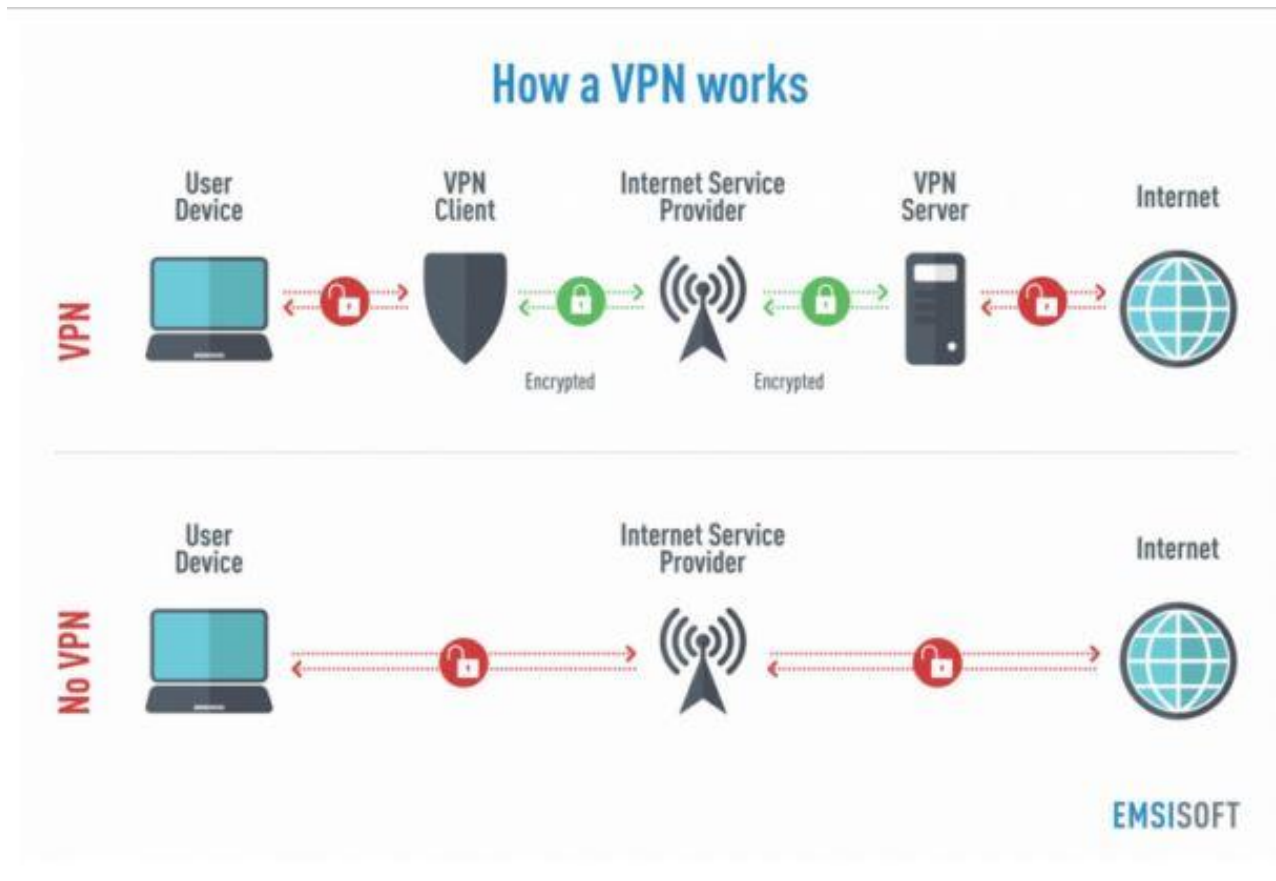
- **Connect to websites securely.** If you see “https” or a lock in the web address, you have a secure connection to the website. But using https **does not** always mean a website is legit. Scammers know how to encrypt sites, too. They know that people assume “https” means a website is safe — so they’ve started adding it to their websites, as well. Your data is encrypted on its way to the site, but it won’t be safe from scammers operating that site.
- **Use your mobile data. Your mobile data is usually encrypted.** If you’re on the go, don’t have the option of using a secure website, and have no VPN encryption, consider using your mobile data instead of Wi-Fi. This is a good option when you’re putting personal information into apps, since it can be hard to know if they’re encrypted.
- **Don’t access your personal or financial information.** Always assume a public Wi-Fi network isn’t secure.
- **Log in or send personal information only to websites you know are fully encrypted.** To be secure, your entire visit to each site should be encrypted (meaning that the URL starts with https) — from the time you log into the site until you log out. If you think you’re logged in to an encrypted site but find yourself on an unencrypted page (it no longer has the https in the URL), log out right away.

- **Don't stay permanently signed into accounts.** When you've finished using an account, log out.
- **Don't use the same password on different websites.** It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- **Pay attention to warnings.** Many web browsers alert you before you visit a scammy website or download malicious programs. Don't ignore those warnings. **Also keep your browser and security software up to date.**
- **Change your device's settings so it doesn't automatically connect to nearby Wi-Fi.** That way, you have more control over when and how you use public Wi-Fi.
- **Install browser add-ons or plug-ins that can help.** For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. But they still don't protect you on all websites. Look for **https** in the URL to know a site is encrypted.
- **Consider using a VPN.** Virtual private networks, known as VPNs, offer encryption. **However, you learn more about VPN networks before you download or use them.**

*(Federal Trade Commission – Consumer Information)*

## What is a VPN?

VPN stands for Virtual Private Network. A VPN allows you to create a secure connection to another network over the internet. This is done by connecting to a VPN server.



Your Internet Service Provider (ISP) gives your devices an address which is used when you browse the internet.

This IP address uniquely identifies your device and allows it to send and receive information. It's your digital address. But, because your internet connections are not encrypted, everyone else can snoop on you and know what you're doing online and the location of your device.

Your browsing history identifies your likes, dislikes, interests, hobbies, etc. This is valuable information for marketers, data miners, hackers and others.

## → The benefits of using a VPN ←



### **Surf anonymously online**

A VPN provider hides your IP address and replaces it with another one from their system. Because you're sharing this with plenty of other users, you become untraceable online.



### **Protect your digital identity**

Your Internet Service Provider, the authorities, and hackers are always trying to harvest and profit off your data. But with a VPN, you can stop these privacy invasions.



### **Break all geo-restrictions**

Streaming platforms and plenty of other services use your location to determine what content you can access. If you connect to a VPN server in another country, this problem is gone.



### **Download safely**

Making P2P downloads without a VPN isn't safe since your IP address is exposed, and there's no encryption involved. To counter this, a VPN hides your identity and digital life.



### **Unblock websites**

When you deal with digital censorship, a VPN helps you access blocked content. From websites to social media, you can regain and protect your access to information.



### **Get better deals online**

Depending on your location, companies show you different prices. Connect to VPN servers in other countries to find the best deals on plane tickets, hotel rooms, and much more!



### **Stay safe on public Wi-Fis**

The public Wi-Fis you use in cafés, airports, or hotels lack secure setups, so hackers can easily steal your most sensitive information. But a VPN encrypts your connection and keeps you safe.



## Disadvantages of Using a VPN

- It can decrease your internet speed.
- You may experience dropped connections. If this happens, your real IP address may be exposed.
- VPNs aren't legal in some countries.
- The wrong VPN can put your privacy in danger. Free VPNs often keep logs on users and may not protect your privacy.
- The server may be in another country.
- You may choose the wrong kind of VPN. If you want privacy, don't choose a streaming VPN.
- A VPN can't guarantee 100% anonymity.
- VPNs usually don't work with older operating systems.

## Is This Website Secure?



Before entering any personal or financial information into a website, check for “https” or the lock in the browser window. Click on the lock to make sure the certificate is valid and the connection is secure.

Most legitimate sites have gone to this verification as scammers have been using the “https” on the landing pages of fake web pages. However, if you click further into these fake sites, the “https” disappears in the URL. Exit a website immediately if you have this experience.



## What are Cookies?

The main purpose of a cookie is to identify users, save site login details or create customized web pages tailored to the individual's preferences.

Cookies keep track of each time a user visits a site, what they're searching for, what they're buying and generally provide a detailed picture of their online activity on the site.

Cookies are used to improve the user experience and create a more tailored and relevant browsing session.

## Why it's a good idea to delete cookies

- They pose a security threat
- They can slow your browser down
- They store your personal information

## How to delete cookies on your browser

- Go to your browser settings
- Look for privacy or security section
- View the cookies stored in the browser
- Delete the cookies you don't want

# PROTECTING YOUR DATA



Passwords

Cloud Account

Cloud-based Backup Service

External Drive



# PASSWORDS

Passwords are like underwear: Change them often, don't share them and don't leave them lying around.

*Ryan K. Louie*

(And each person – or account – should have their own!)







## **Use a password manager such as LastPass**

You will have to remember only one password, but it should be very strong.

## **Have a unique password for each account**

Hackers can open all the accounts that have the same password. The same goes for modifying a root password that changes with the addition of a prefix or suffix. For example, PasswordOne, PasswordTwo (these are both bad for multiple reasons).

## **Avoid common words and character combinations in your password**

The goal is to create a password that someone else won't know or be able to easily guess. Stay away from common words like "password," phrases like "mypassword" and predictable character sequences like "qwerty" or "thequickbrownfox." Also avoid using your name, nickname, the name of your pet, your birthday or anniversary, your street name or anything associated with you that someone could find out from social media, or a number of other ways.

## **Longer passwords are better: 8 characters is a starting point**

8 characters are a great place to start when creating a strong password, but longer logins are better. Experts advise using a passphrase made up of three or four random words for added security. A longer passphrase composed of unconnected words can be difficult to remember, however, which is why you should consider using a password manager.

## **Avoid using passwords known to be stolen**

Hackers can effortlessly use previously stolen or otherwise exposed passwords in automated login attempts called credential stuffing to break into an account.

## **No need to periodically reset your password**

For years, changing your passwords every 60 or 90 days was a long-accepted practice, because, the thinking went, that was how long it took to crack a password. But Microsoft now recommends that unless you suspect your passwords have been exposed, you don't need to periodically change them. The reason? Many of us, by being forced to change our passwords every few months, would fall into bad habits of creating easy-to-remember passwords or writing them on sticky notes and putting them on our monitors.

## **Use two-factor authentication (2FA) ... but try to avoid text message codes**

If thieves do steal your password, you can still keep them from gaining access to your account with two-factor or multi-factor authentication (also called two-step verification, 2FA or MFA), a security safeguard that requires you enter a second piece of information that only you have (usually a one-time code) before the app or service logs you in. This way, even if a hacker does uncover your passwords, without your trusted device (like your phone) and the verification code that confirms it's really you, they won't be able to access your account.

While it's common and convenient to receive these codes in a text message to your mobile phone or in a call to your landline phone, it's easy for a hacker to steal your phone number and then intercept your verification code. Experts recommend verification apps as a good alternative. (Check out Microsoft Authenticator in the App Store on your mobile as an example. It's highly rated and free.)



## **Never use the password you've picked for your email account at any online site**

If you do, and an e-commerce site you are registered at gets hacked, there's a good chance someone will be reading your e-mail soon.

## **Avoid using simple adjacent keyboard combinations**

For example, "qwerty" and "asdzxc" and "123456" are horrible passwords and are easy to crack.


## **Do not use words that can be found in the dictionary**

Password-cracking tools freely available online often come with dictionary lists that will try thousands of common names and passwords. If you must use dictionary words, try adding a numeral to them, as well as capital letters or punctuation at the beginning or end of the word (or both!).

## **Do not choose passwords based upon details that may not be as confidential as you'd expect**

Information such as your birth date, your Social Security or phone number, or names of family members is available to hackers.

## **Create unique passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters.**



There are several online third-party services that can help users safeguard sensitive passwords, including LastPass, DashLane, and 1Password that store passwords in the cloud and secure them all with a master password.


If entrusting all your passwords to the cloud isn't comfortable for you, consider using a local password storage program on your computer, such as Roboform, Dashlane or iPassword. Again, take care to pick a strong master password, but one that you can remember. If you forget the master password, you are pretty much out of luck.

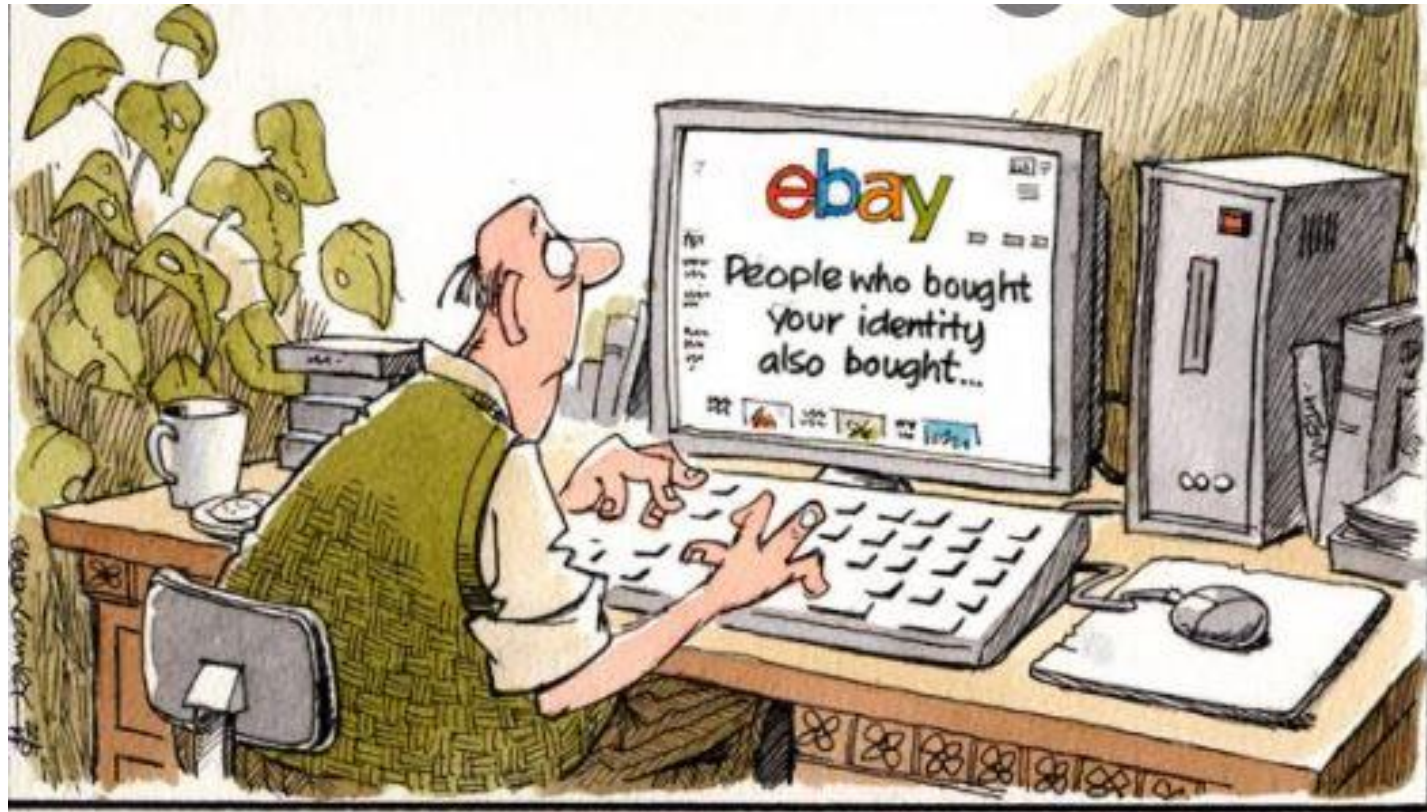
OR...you can write your passwords in a notebook that you keep in a secure place near your computer.

## MORE TIPS TO PROTECT YOURSELF AGAINST CYBER ATTACKS

- Limit the personal information you share online. Change privacy settings and do not use location features.
- Keep software applications and operating systems up-to-date.
- Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true or needs your personal information. Think before you click. When in doubt, do NOT click.
- Protect your home and/or business by using a secure Internet connection and Wi-Fi network.
- Don't share PINs or passwords. Use devices that use biometric scans when possible (e.g. fingerprint scanner or facial recognition).
- Check your account statements and credit reports regularly.
- Be cautious about sharing personal financial information, such as your bank account number, social security number, or credit card number. Only share personal information on secure sites that begin with https://. Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.



- 
- Back up your files regularly in an encrypted file or encrypted file storage device.
  - Use two- or multi-factor (2FA or MFA) authentication whenever possible. E-mail or authentication apps are recommended.
  - Do not click on links in texts or emails from people you don't know. Scammers can create fake links to websites.
  - Remember that the government will not call, text or contact you via social media about owing money or receiving economic impact payments.
  - Keep in mind that scammers may try to take advantage of financial fears by calling with work-from-home-opportunities, debt consolidation offers and student loan repayment plans.
  - If you notice strange activity, limit the damage by immediately changing all your internet account passwords.
  - Consider turning off the device. Take it to a professional to scan for potential viruses and remove any that they find. Remember: A company will not call you and ask for control of your computer to fix it. This is a common scam.



Don't let this be you!!

# CLOUD ACCOUNTS (EXAMPLE: MICROSOFT OFFICE 365)



## Microsoft Office 365

- Installed and web-based apps subscription is about \$100/year for the Family Plan. Can be used by 2 – 6 people. Has 1TB of storage space per person. Works on Windows, Mac, iOS and Android devices.
- Continuously updated; no need to purchase new software.
- Free version includes Word, Excel, PowerPoint, OneDrive, Outlook, Calendar and Skype but functions are limited. Web-based only so you'll still need installed Office software.
- Protects files from fire, flood, theft, hard drive ransom ware or hacking.
- 365 One Drive encrypts all files but for sensitive files, a third-party encryption software program on your computer with multi-factor authentication is recommended. Encrypt sensitive files before moving them to One Drive.

# CLOUD-BASED BACKUP SERVICE (EXAMPLE IDRIVE)



IDrive® Personal



~~\$79.50/year~~

**\$59.62**

first year

One user, Unlimited computers

5 TB Storage

Backup drives allow you to recover your data in the event your computer crashes or is otherwise damaged or if you have the misfortune of being a ransomware victim.

Computers can be set to back up on a daily schedule and you can monitor all covered devices from one web-based account. (Below)

<input type="checkbox"/>		DESKTOP-OSB	SchoolBell		Online	DESKTOP-OSB	13 hours ago	Success		6.7.3.43	10/01/2021		
<input type="checkbox"/>		ALSLC-FINANCE	Office-LDT		Online	ALSLC-FINANCE	16 hours ago	Success		6.7.3.43	10/01/2021		
<input type="checkbox"/>		USER-LTC	user		Online	USER-LTC	14 hours ago	Success		6.7.3.43	10/01/2021		

# EXTERNAL HARD DRIVE

External hard drives allow you to save your data on a portable drive. With most, you'll have to drag and drop your files manually as opposed to the automatic cloud-based backup, though some do have the auto backup feature. Most new external drives come with 2T (terabytes) of memory which is plenty for storing photos and videos.

External drives need to be replaced every few years as they can become corrupted. They also should be stored in a secure place when not in use.



Seagate Portable 2TB  
External Hard Drive  
Portable HDD – USB 3.0  
for PC, Mac, PS4, &...  
★★★★☆ 163,357  
\$54.99 ✓prime



WD 2TB My Passport  
Portable External Hard  
Drive HDD, USB 3.0, USB  
2.0 Compatible, R...  
★★★★☆ 25,905  
\$64.73 ✓prime



Seagate One Touch SSD  
2TB External SSD  
Portable – Black, speeds  
up to 1030MB/s, wit...  
★★★★☆ 1,428  
\$299.99 ✓prime



Toshiba Canvio Basics  
2TB Portable External  
Hard Drive USB 3.0,  
Black - HDTB420XK3AA  
★★★★☆ 40,115  
\$52.74 ✓prime



Seagate IronWolf 12TB  
NAS Internal Hard Drive  
HDD – 3.5 Inch SATA  
6Gb/s 7200 RPM 25...  
★★★★★ 12,926  
\$299.99 ✓prime





THANK YOU!