WFG National Title

SAFE Advisor

A quarterly publication from WESTprotect

May 2021

Avoiding Online Scams and Identity Theft

Technology allows us to connect with anyone, anywhere in the world, no matter where we are. We can bank and shop online and even control our televisions, homes, cars, and all of our IoT devices from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams. By using the Internet, we continually need to make decisions that affect our security.

To help protect yourself against these online threats, here is a list of common Internet frauds for this past year from the Federal Trade Commission.

- **Imposter scams** were the top fraud of 2020. Scammers showed up wearing many different masks — from that of a government official to a known business, to a dear family member or friend. The FTC got nearly 500,000 reports of imposter scams, and people reported losing $1.2 billion, with a median loss of $850. Government and business imposter scams were also among the top categories of COVID-19 and stimulus-related reports, proving once again that scammers follow the headlines.
- **Identity theft** is the illegal use of someone else's personal information in order to obtain money or credit. How will you know if you've been a victim? You might get bills for products or services you didn't purchase. Your bank account might have withdrawals you didn't expect or have unauthorized charges on your credit cards. You may even see new accounts opened in your name that you did not authorize. You may be unexpectedly denied for a credit application.
- **Phishing attacks,** using legitimate-looking emails that encourage people to click on a link or open an attachment, are a favorite of cybercriminals. The email they send can look like it is from an authentic financial institution, e-commerce site, government agency, or any other service or business.
- **The phone** is still the top way that scammers are reaching us — both through phone calls and text

continued on next page

WFG National Title

SAFE Advisor

A quarterly publication from WESTprotect

continued from previous page

messages. There was a sharp increase in the number of reports saying that scammers contacted them by text message. Many of these scams were luring people to click on links with promises of stimulus relief, economic relief or loans for small businesses, or "waiting packages."

Simple Guidelines:

There are many steps consumers can take to avoid becoming victims of identity theft or online scams.

- **When in doubt, throw it out.** Links in email, tweets, posts and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, it's best to delete it.
- **Think before you act.** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or asks for personal information.
- **Make passwords long and strong.** Create a password with ten characters or more that uses a combination of numbers, letters, and symbols.
- **Protect your personal information.** Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself.
- **Use multi-factor authentication (MFA).** Using stronger authentication requires that you use your password in conjunction with an additional piece of information (such as a PIN sent to your mobile device) to verify your identity. If a cybercriminal tries to access your account and has captured your password, they still cannot get account access without the second component.
- **Unique account, unique password.** Create unique passwords for each account. Keeping separate passwords for every account helps thwart cybercriminals.

Banking

- Do not access your personal or bank accounts from a public computer or public Wi-Fi network, such as the public library. Not only can cybercriminals potentially gain access to your accounts through public Wi-Fi, but strangers can easily shoulder surf and see the sensitive information on your computer or mobile device screen.
- Don't provide personally identifiable information such as your bank account number, Social Security number, or date of birth, or any non-public personally identifiable information to unknown sources.

Shopping

- Make sure the website address starts with "https" - the "s" stands for secure.
- Look for the padlock icon at the bottom of your browser, which indicates that the site uses encryption.
- Type new website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

WFG National Title

SAFE Advisor

A quarterly publication from WESTprotect

May 2021

Protection from Malware

Malware poses a threat to anyone using a laptop, tablet, or cell phone. According to leading researchers, it's estimated that 560,000 new malware threats are developed/discovered daily. As a company, it is everyone's job to keep sensitive data safe, just as you would keep your own sensitive data safe. We have various anti-virus programs that help us defend our computers, but people are our most valuable front-line defense in an ever-changing landscape.

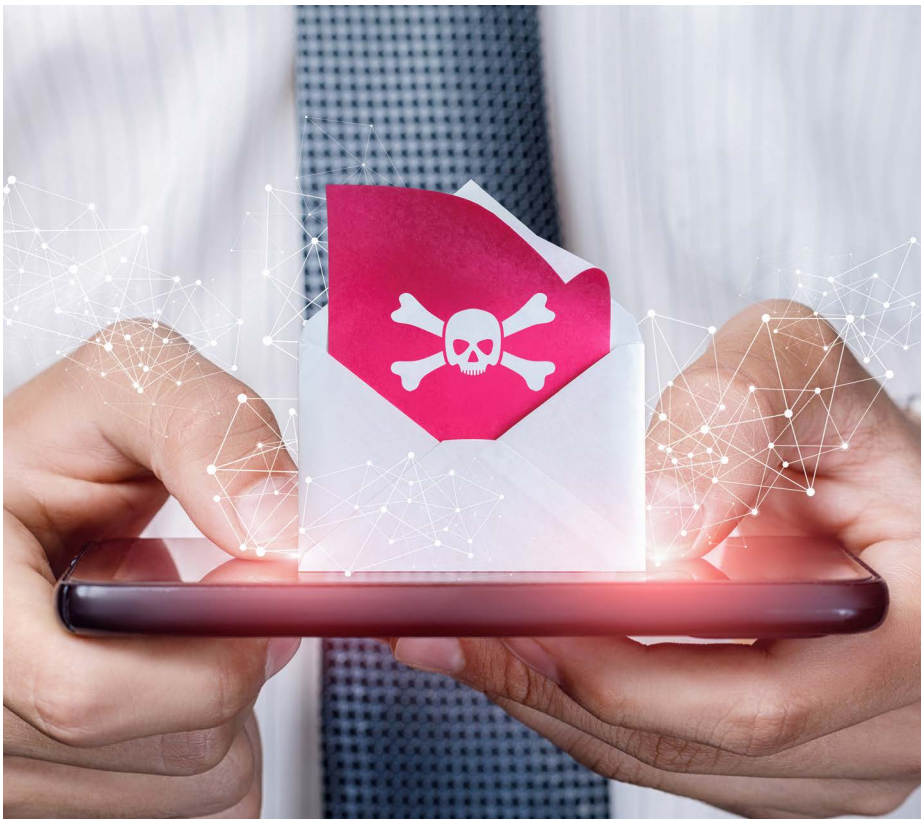
Malware is an abbreviated form of "malicious software." Software is considered malware based on the intent of the creator rather than its actual features. Below is a list of some of the different types of malware and what they do.

- **Ransomware** – disables victim's access to data until a ransom is paid. However, there is no guarantee that you will get your data back if you do pay a ransom.
- **Spyware** – collects user activity data without their knowledge, including passwords, pins, and payment information.
- **Adware** – tracks a user's surfing activity, then serves unrequested advertisements and creates a profile of the user, including who their friends are, what they purchase, where they travel, etc.
- **Trojans** – disguises itself as desirable software. Once downloaded, the Trojan can take control of the victim's system for malicious purposes. It can hide in games, apps, even software patches or embedded attachments in phishing emails.
- **Worm** – installs itself and spreads through a network by replicating itself. Once in place, it can steal sensitive data, conduct ransomware and other attacks.
- **Virus** – installs itself into an application. Once the application is run, it can steal sensitive data, conduct ransomware, and other attacks.
- **Rootkits** – gives hackers remote control of a victim's device.

continued on next page

continued from previous page

- **Keyloggers** – monitor users' keystrokes and are used to steal password data, banking information, and other sensitive information.
- **Bots/Botnets** – bots (a bot is an infected and controlled computer) are used in large numbers to create a botnet to launch a broad flood of attacks to interrupt supply chains, steal sensitive information, and conduct corporate sabotage. The largest known botnet included up to 2.5 million bot computers.
- **Mobile Malware** – infects mobile devices with many different types of malware (the same as listed above for computers). These attacks have increased 50% since last year.



How do you get infected?

Phishing – This is one of the most popular and easiest ways to get infected, with 92% of malware delivered through email. Of these emails, about 90% of them distribute malware through macros in the attached documents. Someone could send you an email with a link or an attachment, or a web address for you to visit, all of which can infect your computer with malware. When opening an attachment in an email, you may get a prompt to click to enable content to view it, but this will enable a macro which then downloads the malware to your computer. Don't enable macros!

Downloading Free bundled software programs - The software company will partner with others to provide enhancements like toolbar add-ons to their programs, but which may also be hiding spyware or worse. Any download of media, apps or browser extensions can also install malware on your computer, cell phone, or tablet.

Removable storage – Items like CDs, DVDs, and USB sticks can have malware that is run automatically and can infect computers when they're connected, sometimes even when the user isn't logged in. Any USB device - even a keyboard, mouse, or USB chargers - can be constructed to access a computer as a different device. For example, a keyboard can be programmed to run commands or load malware as if the user ran them, or a network card could intercept network traffic and otherwise do anything any other USB device can. Just plugging these into your devices can infect them, along with anything else you then plug into it.

Scareware - As the name suggests, these scary pop-ups tell you your computer is infected with malware, and you need to take immediate action to clean it to avoid further damage. However, the link they provide to clean the supposed malware is the malware.

continued on next page

continued from previous page

How can you avoid being infected?

Follow the usual advice you have heard time and again (there is a reason it gets repeated):

- Make sure you have anti-virus programs on all your devices
- Make sure your operating systems, web browsers, and security software are current
- Do not download files from unknown sources
- Disable Macros from running without a notification when opening documents
- Enable multi-factor authentication on all your online accounts
- Disable removable storage auto-play
- Look at what controls your operating system has to protect you
- Do not open files or click on links in email from senders you do not know
- Stick to well-known websites and avoid visiting any suspicious sites
- Remove any unwanted or unused applications on your devices

What are some of the signs that may indicate you could be infected?

- You start seeing suspicious pop-ups ads or notifications.
- Your computer is no longer responsive, is unusually slow or sluggish, or crashes over and over.
- You see emails in your Sent messages folder - messages you did not send.
- You try to open files or folders and find they are now locked.
- You have new icons for apps or programs you did not download.

But don't panic just yet - there could be something else causing some of these issues. If you suspect your computer is infected with malware, report it and have it checked right away.

WFG National Title

SAFE Advisor

A quarterly publication from WESTprotect

May 2021

Just Delete It, and It's Gone, Right?

Whether you have decided to upgrade to a new computer, cell phone, or tablet, or you've decided to clean out all the old files and data on your devices for more storage space or better security, you should make sure you do it right.

Just highlight the name of a file and press the Delete key. That file is gone for good, right? Not necessarily. Most systems only remove the link to the file. It's still there until another file is saved over the older "deleted" data.

Deleting old data . . . permanently

Files that are never permanently deleted from old computers and devices are a gold mine for hackers. Using the latest data recovery technology, they can recover even the data and files you may have thought you deleted. Here's are some tips for making sure that "delete" really means delete.

Digital Data

Most organizations have policies and procedures in place for disposing of old computers and storage media, but how do you handle your own devices? Be sure to use a program that deletes the data, "wipes" it from your device, and then overwrites it by putting random data in place of your information so that it cannot be retrieved.

Smartphones

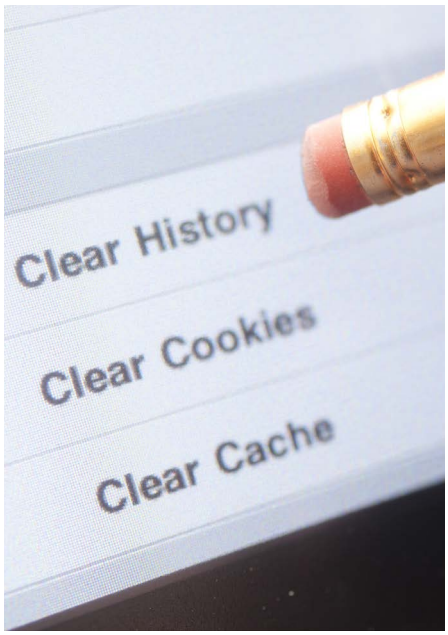
Your phone may have sensitive data even if you don't store any data files on it. This sensitive data can include emails or text messages, pictures, voicemail, or documents left open in your browser. If it's time to upgrade to a newer phone, don't just get rid of your old one or drop it in a recycle bin. Some devices have a remote wipe feature in case they get lost or stolen. Use that to scrub your old phone before getting rid of it, or you can use a reputable data destruction service.

continued on next page

continued from previous page

Cloud

Getting rid of data in your cloud accounts is more complicated. If, for example, you quit using an online service, data from your past usage is still stored by that provider. At a minimum, you should close your account. If you didn't check out the provider's Privacy Policy or Terms of Use when you signed up for their services, you might also need to contact customer support to find out when closed accounts (and any data associated with that account) are permanently deleted. There are also state laws that you should also look to for guidance when requesting that companies delete your personal information.



Whether you are replacing your old digital devices, or just cleaning out your current ones, knowing how to properly get rid of unwanted (but maybe sensitive) data is an excellent process to have. The final step is to check that all the security features and settings on all those devices are set up and working at your comfort level. Good job!

It's almost summer, so get out there and enjoy - securely and safely!