



Cybersecurity for Everyone

Overview: Take your computer and Internet experience to the next level. Learn about Internet safety features, backing up your devices, and privacy issues. Learn tips to keep your computer, yourself, and your loved ones, safer while surfing.

Student Skill Level: Intermediate/Advanced

Requirements:

- Good mouse skills (ability to move the mouse on the computer screen and click or double click as required with minimal assistance)
- **Internet Basic Class** OR Familiarity with using the Internet – opening the program, navigating to web sites, basic search skills

Objectives:

- The student will be able to:
 - Discuss various ways Web sites show they have a secure connection
 - Discuss keeping devices safe: backup and more
 - Define and discuss network threats aimed at personal computers
 - Recognize Apps parents should look out for
 - Discuss Privacy: Browsers and search engines – what is most private for you?
 - Discuss Artificial Intelligence (Example: Use ChatGPT to learn about terms of service)
 - Understand how app stores (Apple and Google) have changed regarding app safety
 - Discuss scams
 - Explore popular web sites:
 - Youtube
 - Twitter/X
 - Library Catalog and digital media



Secure Web Site Example

I want to point out the standard security features of this site. Not every Web site **NEEDS** to be secure. It's only very important when **you** are **giving out personal information** – name, social security number, etc. It is imperative that you check a site's security **BEFORE** you enter personal data – even from a well-known company.

All legitimate businesses have a great interest in keeping your information secure. This is done by a two-part process: **first**, by ensuring that your computer is in fact connected to the **correct server**, and **second**, by **scrambling data sent** over the Internet in such a way that if anyone tried to steal it, all they would find is meaningless, random information.

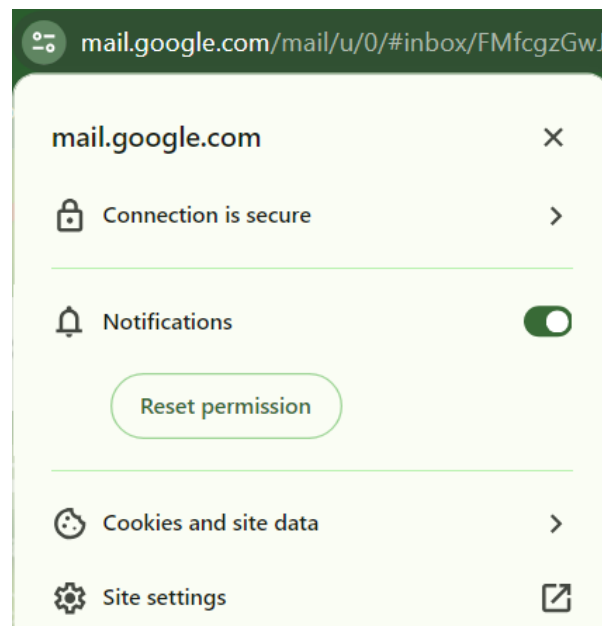
Check if a site's connection is secure

Chrome helps you browse more securely by alerting you when it detects a site that may be unsafe to visit. When a site may be unsafe, Chrome changes the icon next to the site address.

1. In Chrome, open a web page.
2. To check a site's security, to the left of the web address, check the security status symbol:
 - 🛡️ Default (Secure)
 - ⓘ Info or Not secure
 - ⚠️ Not secure or Dangerous
3. To find a summary of the site's privacy details and permissions, click the icon.

<https://support.google.com/chrome/answer/95617?hl=en>

This is what you see when you click the icon in the upper left corner.



Default (Secure)

Information you send or get through the site is private between you and the site.

Even when connected to a site securely, always be careful when you share sensitive or personal information. Check the site name in the address bar to make sure you're on the site you want to visit.

Info or Not secure

The site doesn't use a private connection. Someone may be able to view and change the information you send and get through this site.

To resolve this issue, the site owner must secure the site and your data with HTTPS.

Not secure or Dangerous

We suggest you don't enter any private or personal information on this page. If possible, don't use the site.

Not secure: Proceed with caution. Something is wrong with the privacy of this site's connection. Someone might be able to find the information you send or get through this site.

Dangerous: Do not use this site. If you get a full-page red warning screen, the site has been flagged as unsafe by [Safe Browsing](#). The site can misuse or abuse any information it receives, and could potentially attempt to install harmful software on your computer. When you use this site, it puts your privacy and security at risk.

<https://support.google.com/chrome/answer/95617?hl=en#zippy=%2Cdefault-secure%2Cinfo-or-not-secure%2Cnot-secure-or-dangerous>

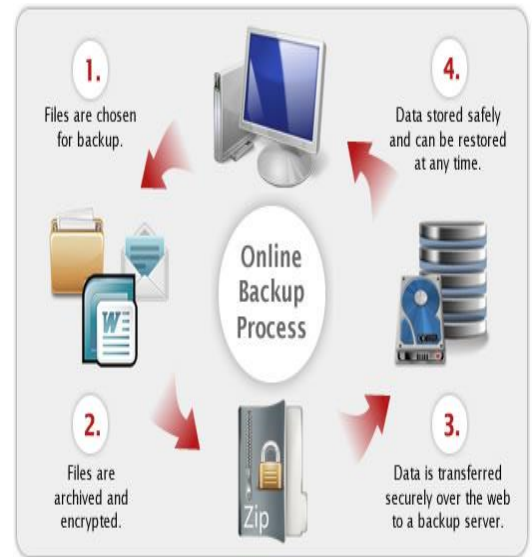
Keeping your Computer Device Safe: Multiple Issues

Mr. Christopher Barnatt (2017) has an excellent online article on keeping devices safe. He discusses multiple issues with device security, including:

"The range of means by which the security and integrity of computing resources can be threatened is very broad, and encompasses:

- Operator error (for example a user inadvertently deleting the wrong file).
- Hardware or media failure (either as a result of wear-and-tear, old age or accidental damage).
- Theft or sabotage (of hardware and/or data or its media).
- Hackers (who obtain unauthorised online access via the Internet).
- Malware (any form of virus, and including "Trojan" e-mail attachments that users are encouraged to open).
- Power surges and/or outages (which are one of the most common means of hard disk corruption and hardware damage).
- Flood, fire, storm or other natural disasters.
- Fraud or embezzlement.
- Industrial espionage.
- Terrorism."

“Whilst physical threats need to be protected against, **most data is lost or corrupted following user error or hardware failure**. The best defence against this is an **appropriate back-up strategy**, triggered on both a time and event basis and with appropriate physical resilience. In other words, users need to ensure that they take regular back-ups at regular intervals and before and after making key data changes. They also need to store multiple back-ups on different media in different locations. **There is no such thing as a permanent store of any form of computer data. Nor is any storage location entirely safe** (although the cloud data centres run by Google, Amazon, IBM, Microsoft and other computing industry giants are pretty well protected these days!).”



Backing Up your Files

There are dozens of ways to back up your files. Some are free (copy to an external hard drive or flash drive) and some are paid. The “free ways” are great, because they’re free. The “paid ways” are great because they are **automatic** and that’s a big advantage.

“Back Up to an External Drive: If you have an external USB hard drive, you can just back up to that drive using your computer’s built-in backup features. On **Windows, use File History**. On **Macs, use Time Machine**. Occasionally connect the drive to the computer and use the backup tool, or leave it plugged in whenever your home and it’ll back up automatically. **Pros:** Backing up is cheap and fast. **Cons:** If your house gets robbed or catches on fire, your backup can be lost along with your computer, which is very bad.” (Hoffman, 2017).

Back Up Over the Internet: If you want to ensure your files stay safe, you can back them up to the internet with a service like BackBlaze. **BackBlaze** is the well-known online backup service we like and recommend since CrashPlan no longer serves home users, but there are also competitors like **Carbonite** and **MozyHome**. **For a low monthly fee (about “\$5 a month), these programs run in the background on your PC or Mac,** automatically backing up your files to the service’s web storage. If you ever lose those files and need them again, you can restore them. **Pros:** Online backup protects you against any type of data loss—hard drive failure, theft, natural disasters, and everything in between. **Cons:** These services usually cost money...and the initial backup can take much longer than it would on an external drive—especially if you have a lot of files.” (Hoffman, 2017).

Threats: Malware

“Malware, short for *malicious software*, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code” (Wikipedia, 2010). “Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses/worms, trojan horses, most spyware, dishonest adware, or crimeware” (2010). These programs are created by computer programmers usually known as hackers.

Malware is installed on a computer either through **technical stealth** (hackers create computer programs to entirely mask the malicious software) or **social engineering** (getting unsuspecting computer users to divulge confidential information – a con game.)

Threat:

Virus/Worm - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer. Some will use the infected computer's Internet connection to move to a new computer for infection

Trojan Horse - a program that appears desirable but actually contains something harmful (for example, a user chooses to download a game from somewhere and not only gets the game but also the malicious software).

Spyware – Secretly installed computer software that obtains information from a user's computer without the user's knowledge or consent.

Threat Management: Keeping a Computer Safe

Every computer should have certain programs running for protection against common security threats:

Firewall – the first line of defense for your computer. Any firewall program is designed to keep “guests” out of your computer. It “can be ... a software application that monitors the “perimeter” of the network to act as the gatekeeper for all incoming and outgoing traffic” (Bradley, 2011). Common free firewalls are Windows Firewall and ZoneAlarm; you may pay for firewalls from CA, Norton, McAfee, or Internet service providers such as Verizon or Spectrum.

Antivirus Software – Whatever antivirus program you choose to run on your computer, **keep it up-to-date**. That is the single best thing you can do to keep your computer running smoothly. Any antivirus

Anti-Spyware - Helps protect against a wide range of spyware threats.

NOTE: Even the best security systems can be breached from time to time. The idea is to keep your computer as safe as you think reasonable – knowing your risks and keeping safe without breaking your wallet.

Common providers of **Internet Security** programs for all computer types:

PAID:

- Norton (Symantic Co.)
- McAfee
- Trend Micro

FREE:

- AVG
- Avast
- Windows Defender (Comes **pre-installed** on all Windows 10 and newer computers)

These Internet Providers have their own security packages available for purchase:

- Verizon (FiOS and DSL)
- Spectrum (cable)

****These are just a few of *many* different providers and this list does not constitute an endorsement of any kind.****

20 Apps Parents Should Know



20 APPS PARENTS SHOULD KNOW



SNAPCHAT



Snapchat is one of the most popular apps. Promotes disappearing photos, videos and stories but doesn't prevent screenshots. Snap Map can let others know your location.

TIKTOK



TikTok is a very popular app. Used for sharing short videos with very limited privacy controls. Users are vulnerable to explicit material.

DISCORD



Discord is a messaging platform for kids to hang out and talk about gaming. Features chat rooms, direct messaging, voice chat and video calls. Can expose kids to inappropriate or explicit content.

ROBLOX



Roblox is an online gaming platform that has a chat function. Underage users have reported solicitation from sexual predators.

LIVEME



LiveMe is a live-streaming video app for users to share videos. Uses geolocation so a broadcaster's exact location can be seen by users. Users can earn "coins" to "pay" minors for photos.

OMEGLE



Omegle is an online chat site that does not require registration. Users can chat anonymously via video, private chat, or group chat. Child pornography has been an issue with this site.

CALCULATOR%



Calculator% can hide photos, videos, files, and browser history. Only one of several secret apps used for this purpose.

MEETME



MeetMe is a dating social media app. Allows users to connect with others based on geographic proximity. Users are encouraged to meet in person.

YUBO



Yubo is a popular app among teens. Called "Tinder for teens" it is designed to allow teens to flirt with each other. Has been frequented by sexual predators.

WHATSAPP



WhatsApp is a messaging app where users can send texts, photos, voicemail, make calls, and video chat worldwide. Uses an internet connection and can track location if enabled.

KIK MESSENGER



Kik Messenger allows anyone to contact a direct message a child. Kids can bypass traditional text messaging features. Kik gives users unlimited access to anyone, anywhere, anytime and doesn't track phone numbers of users.

BADOO



Badoo is a dating and social networking app to chat, share photos and videos, and connect based on location. Intended for adults, teens have been known to create profiles.

ASK.FM



Ask.fm is known for cyber bullying. Users are encouraged to allow anonymous people to ask them questions.

SKOUT



Skout is a location-based dating app and website. Users under 17 are unable to share private photos, however kids can easily falsify their age.

YIKYAK



YikYak is an anonymous chatting app that lets users within a five-mile radius read publicly posted messages. Known to be a breeding ground for bullying and promotion of sexual assault and violence.

YARN



Yarn is a reading app that tells stories via fake text messages. Topics can be scary or sexual in nature. Can also watch short videos or listen to audio.

MONKEY



Monkey is a video chatting and social media app that allows kids and teenagers to connect with strangers online. Has a video chat feature and duo chat feature. Actively pushes its users to record themselves live.

WHISPER



Whisper is an anonymous social network that promotes sharing secrets with strangers. User location is revealed so people can meet up.

BUMBLE



Bumble is a popular dating app similar to Tinder, however women are required to make the first contact. Kids have been known to create fake accounts and falsify their age.

HOOP



Hoop is an app that connects with Snapchat to allow users to "make new connections". Known as "Tinder meets Snapchat" Hoop allows kids as young as 12 to form connections with total strangers. Hoop claims users over 18 won't be shown kids' profiles.

This list is not exhaustive. These and other apps can be used as grooming tools by online predators.
(Updated 09/2022)

SPECIAL ATTENTION: SNAPCHAT is very popular and kids use it a lot. Notifies users when screenshots are taken or when snaps are saved, but can simply be recorded by another device and the "snapper" is unaware of it. Possible to delete chats and snaps (pictures) but if the screen is recorded by another device, the person (usually a kid) will have no idea, and the information is out there forever.

TIKTOK: Algorithm is scary quick in noting what a user watches, pauses, or just glances at and will serve up similar videos almost instantly. US companies like Instagram and Facebook do this, but not as quickly or as obviously, because these are US companies and have a primary audience who expects a certain level of privacy. With TikTok, Chinese (who were the first or primary audience) have no such expectation.

CALCULATOR%: is a "secret app/secret folder" that allows people to hide photos, videos, and even browser history on a device. It is easy to overlook because it just looks like a calculator and therefore nothing important.

PLEASE NOTE: These are not necessarily "bad" applications to use, just apps to be aware of if you see them on someone's phone. Anyone can use these apps responsibly and have no issues.

Privacy for You: The Brave Browser and Leo Search Engine

THE BRAVE BROWSER: Brave is available for download on tablets and smartphones, as well as download from the web on Windows and Apple computers. It is currently the most private way to search the web and has its own search engine, named “Leo” (hence the lion logo).



The following is from www.brave.com:

“Brave blocks third-party ads on every website. That’s video ads, search ads, social media ads, and more. And those annoying “Accept cookies?” pop-ups? Yeah, we block those too.”

“Unparalleled Privacy: Shields against tracking and fingerprinting. A premium VPN that can encrypt every connection no matter where you are. On-by-default Global Privacy Control to stop websites from selling and sharing your data. All this (and more) in one ridiculously easy package.”

“Who owns Brave? The Brave Browser, Brave Search, and all their various features are made by Brave Software Inc, an independent, privately-held company. Brave is not beholden to any other tech company, and works every single day to fight Big Tech’s terrible privacy abuses. Brave exists to help real people, not some faceless tech company.”

How does Brave make money? A type of cryptocurrency called “BAT” or Basic Attention Token. BAT is a digital asset, and a key (but totally optional) part of the Brave Rewards ecosystem. Here’s how it works:

Brave Rewards gives you the option to view first-party, privacy-protecting ads while you browse (these ads are from the Brave Private Ads network). If you choose to view them, you earn BAT via the Brave Rewards program.

You can keep BAT like any other digital asset, or use it to tip the content publishers you love. Brave even gives you a secure way to store BAT (and any other asset), with Brave Wallet. And, again, Brave Rewards is a totally optional program.

Other tech companies steal your data to sell ads—to them, you are the product. Brave is different. We think your attention is valuable (and private!), and that you should get a fair share of the revenue for any advertising you choose to view. That fair share is rewarded in BAT.”

“What can you do with BAT? Almost anything! BAT can be exchanged for many different currencies (both fiat and crypto), or used to purchase gift cards. You can use BAT to contribute to websites & content creators you love. You can transfer it to your Web3 wallet and store and swap BAT like any other crypto asset in your crypto wallet. You can even buy NFTs and make in-app purchases in Web3 DApps with BAT.” <https://brave.com/brave-rewards/>

“How is Brave Wallet different from Brave Rewards? Brave Rewards is a feature in Brave that lets you earn BAT for seeing Brave Ads, and lets you support and contribute to websites and content creators. Your BAT earnings are deposited into the **payout account** you connect to your Brave Rewards profile. **Brave Wallet** is a Web3 wallet that allows you to buy, send, manage, and swap almost any crypto asset or **NFT, (a Non-Fungible Token - think of this as the complete opposite of cash. NFTs are completely unique and belong to you. You cannot drop it or get hacked and have someone else use your token. This is where I, personally, stopped setting up a Brave Wallet, because I don’t want to use cryptocurrency.)** Connect other wallets and Web3 DApps, and generally manage your whole crypto portfolio. You can withdraw the BAT you earn from Brave Rewards to a Web3 address you own, such as an address you manage with Brave Wallet. From

there, you can use your BAT with Brave Wallet. <https://brave.com/brave-rewards/#brave-wallet-vs-rewards>.

“**Web3** (also known as Web “three-point-oh”) is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics.” <https://en.wikipedia.org/wiki/Web3>

Artificial Intelligence Example: Terms of Service

CHATGPT: <https://chatgpt.com/> on the web, or download the app from your app store. Look for the correct logo.



I asked ChatGPT to “summarize third party terms of service for Apple products” and this is PART of the answer: “Apple’s products and services often involve third-party terms of service, as many apps, software, and services are created and operated by third-party developers or companies. While the specifics can vary depending on the third-party service or app, here’s a general summary of the typical third-party terms of service related to Apple products:

1. Licensing and Usage

App Store and Apps: When you download an app from the App Store, you're usually agreeing to the third-party developer's terms of service, which govern how you can use the app. These terms may include things like restrictions on redistribution, reverse engineering, or unauthorized copying of the app.” THERE’S A LOT MORE.

This can be a way to get “plain English” that is understandable and not in legal terms.

This is just one example of a possible use for AI. AI Delusions:

<https://www.instagram.com/reel/DN5rxyhDSxK/?igsh=am5rczduaGJ0OWU4> AI Psychosis:
<https://www.psychologytoday.com/us/blog/urban-survival/202507/the-emerging-problem-of-ai-psychosis>

Apple App Store and Google Play Applications (usually for phones and tablets)

Difference between Apple and Android stores and scanning of apps that are now allowed into the stores themselves. Example from 10 years ago: flashlight apps. Apple has a “walled garden” approach to apps they allow on their devices. It can be a bit harder for a developer to get into the App Store on Apple, but that can stifle innovation. Conversely, it was very easy to get an app into the Android store (10 years ago), but now that it is the Google Play Store, there are more protections in place, and all apps are scanned and verified as safer (SAFER) for smartphones and tablets. Nothing is 100% safe. So, Apple has a slightly more open store than it had 10 years ago, and the Google Play Store is a slightly more closed store than it was 10 years ago. Both major companies are trying to balance the access people expect with the safety needed for the devices.

Scams – an introduction

The team at the web site Security.org wrote an amazing piece on current scams that are circulating on the Internet. Remember! The Internet is ALMOST EVERYWHERE nowadays. **It's important to stop and think before clicking or tapping ANYTHING.** Quoting from the 2023 Security.org Team Blog: "In the constantly-evolving digital world, staying informed about the latest internet scams is crucial. This is why we're following up on our 2021 report with all-new insights from 1,026 Americans about their recent experiences with cybercriminals and the latest online schemes. We'll also show you how to spot and stop fraudulent activity online and protect your personal data."

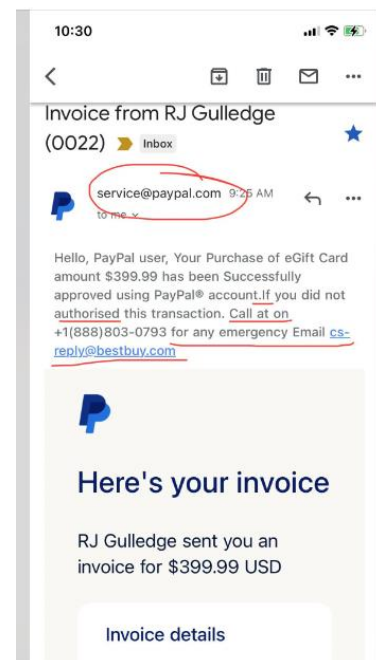
BEST ADVICE: SLOW DOWN, BREATHE, AND THINK. THIS IS WHAT ANY SCAMMER DOES NOT WANT YOU TO DO!



I'm going to quote again from the article, but paraphrase a bit:

"About 76% of Americans use a **peer-to-peer (P2P) app**, such as **PayPal, Venmo, or Zelle**, at least once a week. Though convenient and easy to use, these apps are especially susceptible to scammers since it's typically the users' responsibility to ensure that transactions are legitimate. According to our latest research, 68% of peer-to-peer payment users in 2023 experienced some form of attempted (or successful) scamming activity while using the apps. That's up from 42% of users in 2021. The most common type of scam involves fake prize winnings."

PAYPAL SCAM: Noticed the spelling and grammar mistakes and they never addressed me by my name. Didn't see any pending transaction. Anyone else receive this kind of email? I reported it to phishing@paypal.com. See: https://www.reddit.com/r/Scams/comments/15mh596/just_received_a_suspicious_email_from_paypal/



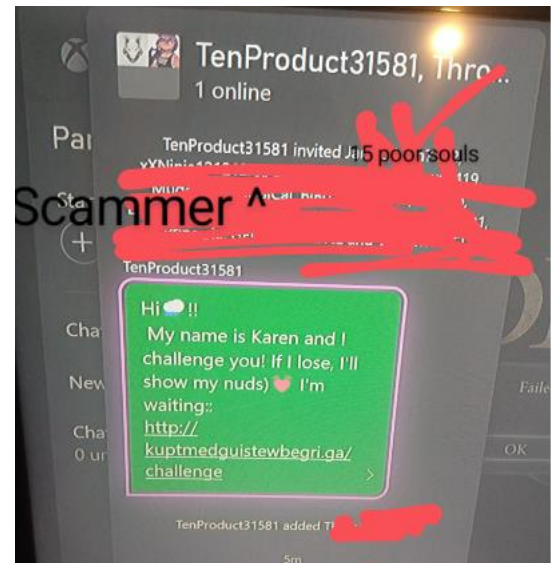
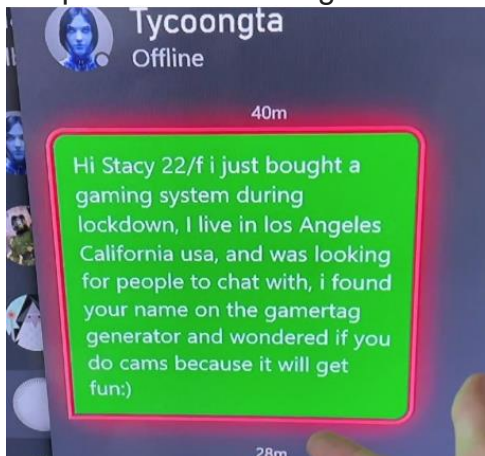
Preventing Peer-To-Peer Payment App Scams

As long as you know the warning signs of peer-to-peer payment app scams, you can use them and safely enjoy their convenience. Follow these tips:

- Use phone numbers, email addresses, or QR codes to verify a recipient's identity before you send money.
- Activate all identity verification options available to you in an app. The recipient of any money transfers must go through various extra steps to pass muster with security.
- When paying a new recipient for the first time, send a \$1 test payment and confirm the correct person received it. This step is even more critical when transferring large amounts of money.
- Move the money you receive in your P2P app to your bank quickly so that Federal Deposit Insurance Corporation (FDIC) insurance kicks in.
- Monitor your P2P accounts routinely. If fraud occurs, you may catch it early enough that the impact on you is minimal.
- Close and delete all P2P apps you do not use."

Fraud in video games is a big problem that spoils the fun for players. Our study found that 37% of gamers have been the target of a gaming scam at least once. People can trick others by selling fake in-game items and money on unauthorized websites. They also make phony game codes and sell them. This cheating hurts gamers by stealing their money and messing with their accounts. As gaming gets more popular, players need to be careful.

Suspicious bot message:



https://www.reddit.com/r/Scams/comments/vb7fv0/this_is_a_new_one_i_can_get_scammed_from_my_xbox/

How to Avoid Gaming Scams

To prevent hacking and phishing while playing video games, take these general precautions:

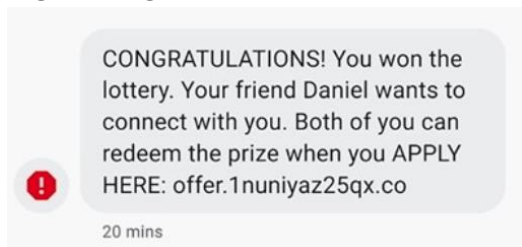
- Avoid clicking on links in emails offering free in-game items; instead, log into the game directly.
- Use strong and unique passwords for your gaming accounts, not ones you've used elsewhere. Never share login, personal, or financial information with people claiming to be gaming staff or online partners.
- Be cautious of too-good-to-be-true offers, especially those promising free access to new games in exchange for personal information or early access at a heavily discounted upfront cost.

Malicious link scams pose a significant threat in the digital landscape, targeting unsuspecting internet users. These scams often involve deceptive emails, text messages, or advertisements that lure individuals into clicking on harmful links that can capture personal data. By clicking these links, people open themselves to identity theft, financial loss, or the installation of malware on devices.

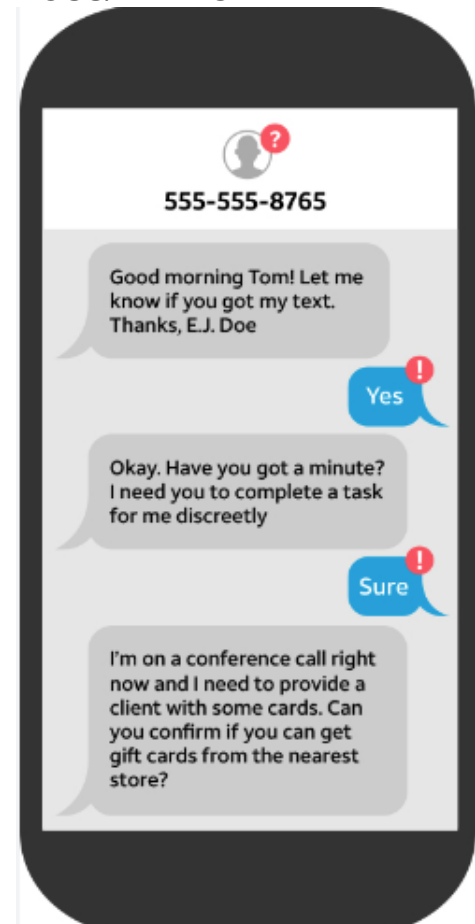
These scams can look like:

- “Oops, wrong number!” texts
- Emails and texts pretending to be from Amazon or other retailers
- Free-gift QR codes
- Tech support scams that gain remote access to your computer
- Late or failed package delivery messages
- Unfortunately, malicious links in text messages are becoming more and more common. 66% of Americans have gotten a text from someone they didn’t know trying to make conversation, and about one in five have clicked on links in text messages from senders they did not know.

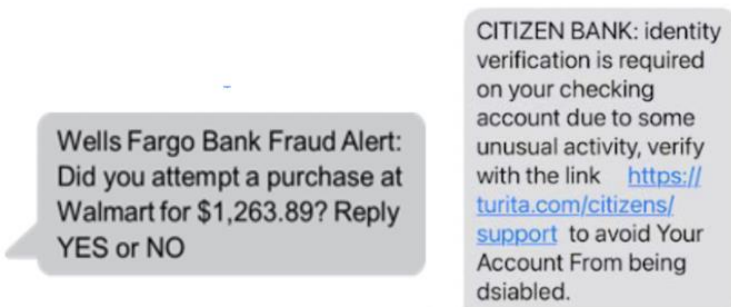
SCAM “LOTTERY WINNER:”



IMPERSONATING A BOSS/MANAGER:



COMMON “BANK TEXT” SCAMS:



Preventing Malicious Link or Phishing Scams

These scams are so insidious in part because they can appear legitimate with messages featuring company logos and the like. Here are a few ways to stop scams before they impact you:

- Ignore messages, emails, and text from people you don't know, and block unknown senders.
- Ignore unexpected emails or texts, including those that claim failed log-in attempts or suspicious activity.
- Watch out for messages with generic greetings such as, "Hello, Dear."

Legitimate companies do not email or text you to update payment details. If you want to access your account to check on billing, never click on a link in a suspected scam message. Instead, type in the URL or Google the company in case you don't remember the URL."

Social Media Shopping Scams

"Shopping through social media is becoming increasingly common. Young adults are especially likely to buy something on a social media platform without leaving the app. However, 22% of people in our study bought something through social media that they never received. This was more likely to happen among younger adults since they spend more time on social media than older adults.

Beware of this common online shopping scam: You click on a product link on social media and purchase on the company's website but receive an email stating that the item is out of stock and you'll get a refund. However, the refund never arrives, and the company remains unresponsive when contacted. Likely, the product never existed, and scammers rely on you not noticing the missing refund.

Thankfully, if you paid with a credit card, you can dispute the charge and recover your money. Before buying from social media, research the business with the keyword "scam" to check for any red flags like unbelievable deals or fake coupons. Always use your credit card for added protection."

Basic Test for Information Reliability: CRAAP

Kaitlyn Van Kampen (2023) summarized this basic information test on the University of Chicago website. It is as follows: "The CRAAP Test is an evaluation method that was designed by librarian Sarah Blakeslee at the Meriam Library California State University, Chico."

C	Currency: The timeliness of the info
R	Relevance: How the info fits your needs
A	Authority: The source of the info
A	Accuracy: Reliability and correctness of the info
P	Purpose: The reason the info exists

1. Currency: The timeliness of the information:

When was the information published or posted?

Has the information been revised or updated?

Does your topic require current information, or will older sources work as well?

Are the links functional?

2. Relevance: The importance of the information for your needs:

Does the information relate to your topic or answer your question?

Who is the intended audience?

Is the information at an appropriate level (i.e. not too elementary or advanced for your needs)?

Have you looked at a variety of sources before determining this is one you will use?

Would you be comfortable citing this source in your research paper?

3. Authority: The source of the information:

Who is the author/publisher/source/sponsor?

What are the author's credentials or organizational affiliations?

Is the author qualified to write on the topic?

Is there contact information, such as a publisher or email address?

Does the URL reveal anything about the author or source? (.com, .edu, .gov, etc)

4. Accuracy: The reliability, truthfulness, and correctness of the content:

Where does the information come from?

Is the information supported by evidence?

Has the information been reviewed or refereed?

Can you verify any of the information in another source or from personal knowledge?

Does the language or tone seem unbiased and free of emotion?

Are there spelling, grammar or typographical errors?

5. Purpose: The reason the information exists:

What is the purpose of the information? Is it to inform, teach, sell, entertain or persuade?

Do the authors/sponsors make their intentions or purpose clear?

Is the information fact, opinion or propaganda?

Does the point of view appear objective and impartial?

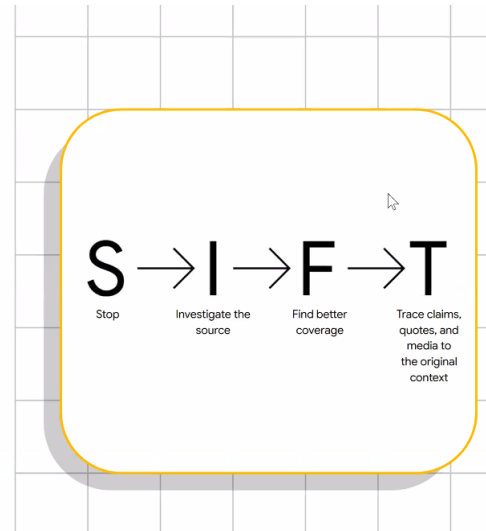
Are there political, ideological, cultural, religious, institutional or personal biases?

SIFT Method

The SIFT method

What is SIFT?

- SIFT is an information literacy framework that takes you through the basics of quick source- and claim-checking.



1. **Stop** – probably the most important and overlooked aspect of research.
2. **Investigate the Source** – multiple ways of doing this – a simple search might yield results
3. **Find better coverage** – this is a sticky wicket as some news articles are created around a single tweet (see “The Twitter/X Effect following this section)
4. **Track claims, quotes, and media to the original content** – again, more searching with different key words will change your search results. Refine, refine, refine!

Any claim, photo, or even your own curiosity can be answered with this method and it seems to work well!

Current News in a Nutshell: The “Twitter/X Effect”

Being the first to report on news is nothing new in the business – reporters and their bosses have been chasing stories from time immemorial. The printing press, telegraph, trains, radios, telephones, video (newsreels in the movie theaters and forward), televisions, and computers have all made marks on the news-gathering industry. **One website that stands head-and-shoulders above them all right now is Twitter, rebranded to “X.”** Pew Research (2021) reports, “News plays a prominent role on Twitter. Overall, 23% of Americans use Twitter, and roughly seven-in-ten U.S. Twitter users (69%) say they get news on the site.... One key area of news people rely on Twitter for is breaking news. Fully 70% of Twitter news consumers say they have used Twitter to follow live news events, up from 59% who said this in 2015.”

Two-thirds of Twitter news consumers have at least some trust in the accuracy of news there

% of U.S. adult Twitter news consumers who trust the accuracy of the news and information they get there ...



<https://www.pewresearch.org/journalism/2021/11/15/news-on-twitter-consumed-by-most-users-and-trusted-by-many/>

The interesting thing about Twitter/X is the fact that it **drives the news cycle**, regardless if YOU use it or not. According to X.blog, “In addition to helping people learn about and share current events, Twitter facilitates the discovery of news outlets and journalists. People regularly follow news-related Twitter accounts, and **more than 80% of young journalists rely on Twitter for their jobs.**”

It goes on to say: “People on Twitter are avid news consumers. Many of them are interested in politics and current events, and they regularly Tweet about it.

- 94% of people on Twitter express interest in current events
- 85% of people on Twitter watch, read, or listen to the news at least once a day
- 83% of people on Twitter Tweet about news
- 3 in 4 people who come to Twitter for news do so at least once a day
- 55% of people on Twitter get their news from Twitter, more than other social media platforms
- 75% of people who come to Twitter for news follow news about politics and current events on Twitter
- In the first 6.5 months of 2022, there were 4.6B Tweets about news in the US (#1) and 10.4B Tweets about news globally (#2)”

This means that newspapers, television, and the Internet itself gets a lot of news and information from X itself. People from all walks of life can post, share, and comment on current events as they happen, which is a first for modern-day news casting. This has both fueled the rise of “citizen journalists” and the ubiquitous use of cameras for anything even remotely interesting. This has positive and negative implications.

News spreads quickly, and that’s great....
But news spreads quickly, and that’s bad, too.


Library Web Site and Digital Items

www.nioga.org

Let’s take a look at the library’s online catalog. **All** the library’s material is shown in the catalog: books, CDs, DVDs, Blu-Rays, magazines, electronic resources, even local history and reference items. By searching the catalog you may find any item the library owns, and with your library card number and a PIN, you may find out what materials are available to request. By requesting an available item (also called placing a hold) you place yourself on a list. When the item becomes available, you are notified by email or telephone, and you may then pick it up at your local library!



Type www.nioga.org in the address bar and press the Enter key on the keyboard.

 www.nioga.org

The catalog home page will appear:

Nioga Library System
Your public libraries in Niagara, Orleans and Genesee counties

Log In | My Account | My Lists | ?

All Libraries | All Fields | SEARCH | Advanced Search

HOME
MEMBER LIBRARIES
DATABASES
TUTORIALS

KIDS CATALOG

Download OverDrive
eBooks, audiobooks & more

Your favorite magazines, available on your device.
Libby

Discover Books with NoveList

Discover Books with NoveList K-8 Plus

NY Times - Hardcover Fiction

Title: **RIGHTEOUS PREY**
Author: John Sandford
ISBN: 9780593422472
Rank (Last Week): 2 (Not Ranked)

Find In My Library

Check with your local public library for details on what services are offered. Library hours may have changed.

Book drops at all locations are available for the return of library materials. All returns will be quarantined for a minimum of 24 hours prior to being checked in and returned to library shelves.

Getting Started

- Log in by clicking Log In or My Account above.
- New library cards use the temporary PIN "changeme".
- Create or change your personal PIN by clicking Change PIN found on the Personal Information tab of My Account.
- If you have problems with your PIN, please contact your local library.

NIOGA Mobile Tech
Libraries lead the way!

Access this catalog using our mobile app!
Download Now: [Android icon] [Apple icon]

select reads
NEW TITLES, STAFF PICKS, TRACK AUTHORS

author check
A FULL-FLEDGED AUTHOR DATABASE

Top of screen:

Search bar: search for any item in the library's collection, including ebooks!

Left side of screen:

Download audiobooks & eBooks: search specifically for ebooks and audiobooks

Libby: a one-stop-app for library ebooks and audiobooks

Discover Books with NoveList: Recommended reading, read-alikes, and more

Discover Books with NoveList K-8 Plus: recommended reading for kids

Middle of screen:

NY Times Bestseller list: find these books in your local library

Hoopla: online music downloads, ebooks, audiobooks, TV shows and movies. Thousands of titles!

Right side of screen:

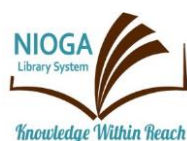
General library information: including how to log in to your library account. "My Account" gives online access to renewals, requests, and hold suspensions

NiogaMobile: tech training classes and schedule

References and Resources

- Barnatt, C. (2017). Computing Security. Retrieved from Explaining Computers Web Site: <http://www.explainingcomputers.com/security.html>.
- Bradley, T. (2011). Introduction to Firewalls. Retrieved from About.com web site: <http://netsecurity.about.com/od/hackertools/a/aa072004.htm>.
- Chui, M., Loffler, M., Roberts, R. (2010). The Internet of Things. Retrieved from McKinsey & Co. Web site: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.
- CNBC. (2013). Youtube Reaches 1 Billion Users Milestone. Retrieved from CNBC Web Site: <http://www.cnn.com/id/100575883>.
- Commonsense Media, Inc. (2006). Internet Survival Tips for Parents and Teachers. Retrieved from Commonsense Media web site: <http://www.commonsense.com/internet-safety-tips/tips-for-parents.php>.
- Commonsense Media, Inc. (2006). Internet Survival Tips for Kids and Teens. Retrieved from Commonsense Media web site: <http://www.commonsense.com/internet-safety-tips/tips-for-kids.php>.
- Easy Desk Software. (2009). Computer Glossary: Home of the Windows Registry Experts. Retrieved from Easy Desk Software Web Site: <http://www.easydesksoftware.com/glossary.htm#Adware>.
- Google Voice Help. (2024). Protect your verification code. Retrieved from Google Help web site: <https://support.google.com/voice/answer/9177797?hl=en>.
- Habas, C. (2022). The Best Parental Control Apps of 2022. Retrieved from SafeWise.com web site: <https://www.safewise.com/resources/parental-control-filters-buyers-guide/>.
- Key Bank. (2009). Information Security Terms Glossary. Retrieved from Key Bank Web Site: <https://www.key.com/html/bank-information-security-glossary.html#R>.
- Hoffman, C. (2017). What's the Best Way to Back Up my Computer? Retrieved from How-To Geek Web Site: <https://www.howtogeek.com/242428/whats-the-best-way-to-back-up-my-computer/>.
- Security Team. (2023). Web of Deception: Online Scams to Avoid in 2023. Retrieved from Security.org web site: <https://www.security.org/digital-safety/new-online-scam-prevention/>.
- Whorley, B. (2012). Does your computer have a Virus? Or is it just SLOW? Retrieved from Yahoo.com web site: <http://news.yahoo.com/blogs/upgrade-your-life/does-pc-virus-just-slow-181117610.html>.
- Dictionary.com Definition: "Toyetic." Retrieved from: <https://www.dictionary.com/browse/toyetic>.
- Facebook.com Definition: "Unpublished Post/Dark Ad." Retrieved from: <https://www.facebook.com/business/help/835452799843730>.
- Hootsuite.com Definition: "Dark Post." Retrieved from: <https://blog.hootsuite.com/social-media-definitions/dark-post/>.
- Kampen, Kaitlyn van (2023). The CRAAP Test. Retrieved from University of Chicago Website: <https://guides.lib.uchicago.edu/c.php?g=1241077&p=9082343>.
- Mitchell, Amy, Shearer, Elisa, and Stocking, Galen. (2021). News on Twitter: Consumed by Most Users and Trusted by Many. Retrieved from Pew Research Center Website: <https://www.pewresearch.org/journalism/2021/11/15/news-on-twitter-consumed-by-most-users-and-trusted-by-many/>.
- Musadiq Bidar, Musadiq. (2021). "An attention treadmill": Lawmakers grill social media companies over use of algorithms. Retrieved from CBSNews.com: <https://www.cbsnews.com/news/social-media-algorithms/>.
- TechTarget.com Definition: "Availability Bias." Retrieved from: <https://www.techtarget.com/whatis/definition/availability-bias>.
- Wikipedia.com Definition: "Filter – Social Media." Retrieved from: [https://en.wikipedia.org/wiki/Filter_\(social_media\)](https://en.wikipedia.org/wiki/Filter_(social_media)).
- Wikipedia.com Definition: "Subvertisement." Retrieved from: <https://en.wikipedia.org/wiki/Subvertisement>.
- X Blog (formerly Twitter Blog). (2022). How many people come to Twitter for news? As it turns out, a LOT. Retrieved from X.Blog Website: https://blog.x.com/en_us/topics/insights/2022/how-many-people-come-twitter-for-news#:~:text=Twitter%20connects%20people%20with%20news,on%20Twitter%20for%20their%20jobs.
- Wikimedia. (2010). Crimeware. Retrieved from Wikipedia Web Site: <http://en.wikipedia.org/wiki/Crimeware>.

Computer Training Program is provided by:



NIOGA LIBRARY SYSTEM

6575 Wheeler Road - Lockport, NY 14094
Phone - (716) 434-6167 Fax - (716) 434-8231



Edited:
2025