
# Online Safety

Bo Ford: Digital Equity Program Manager

New Mexico State Library

# What is the Internet?

- The internet is a global network of interconnected computers.
- The internet allows different devices (like computers, phones, and even TVs) around the world to communicate with each other instantly.
- For many people, the internet is the primary source for information, communication, entertainment, and services—from social media and news to online banking and shopping.
- Since we share so much information online, it's crucial to understand how to protect our personal data.
- What is the Internet? (4 Min Video)

# Importance of Online Safety

Limited access to support services

Dependence on online resources

Increased vulnerability to scams

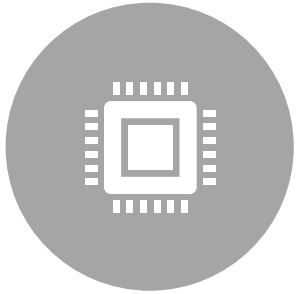
Potential for isolation

Limited awareness to education

# Overview of Online Risks

Common online threats such as phishing, malware, and identity theft.

Malware (short for "malicious software") is software that’s designed to harm or exploit any device, network, or service.



Phishing is a type of online scam where attackers impersonate a legitimate organization (like a bank, social media site, or even a trusted contact) to trick you into sharing sensitive information.

Identity theft happens when someone uses your personal information (like your name, Social Security number, or credit card details) without your permission, often to commit fraud or theft.

# How it Works

Phishing attempts often come in the form of fake emails, text messages, or websites designed to look real. They usually ask you to provide login details, verify your account, or click on a link.

Malware can be installed on your device in many ways—through email attachments, downloads from sketchy websites, or even hidden in ads. Once installed, it can monitor your activities, steal data, or even lock you out of your device.

Attackers might obtain your information through phishing, data breaches, or malware, and then use it to open credit accounts, make purchases, or access other personal accounts in your name.

# How to Avoid It

1

Look for signs like misspellings in URLs, unfamiliar email addresses, or requests for sensitive information. Avoid clicking on suspicious links or downloading attachments from unknown senders.

2

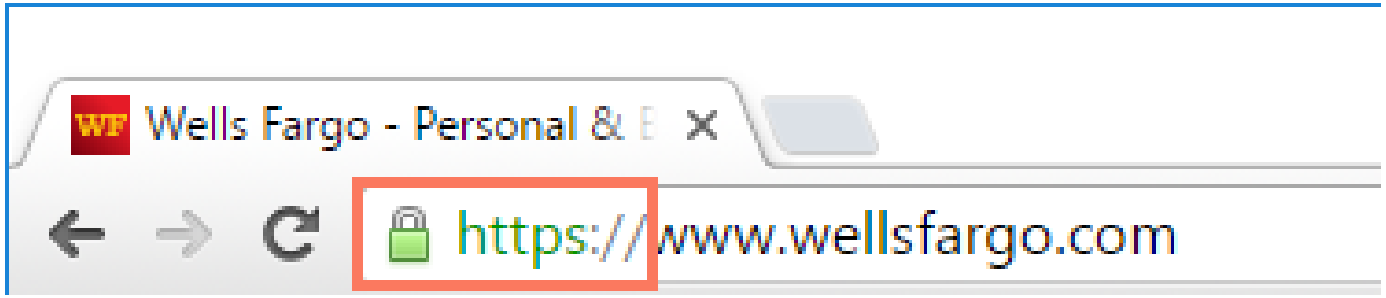
Only download software or files from trusted sources and keep your antivirus software up-to-date. Be cautious of pop-ups or unexpected downloads.

3

Protect sensitive information, monitor your financial accounts regularly, and be careful about sharing personal data online or over the phone.

# Best Practices

- Passwords should be 10 characters or more with letters, numbers, and symbols, and not include any obvious personal information or common words.
  - (m#P52s@ap$V)
- Check the web address for clarity.
  - (www.wellfargo.com vs www.wellsfargo.com)
- Check to see if the lock symbol is in the address bar.



# Avoid Suspicious Links

You've won a prize.

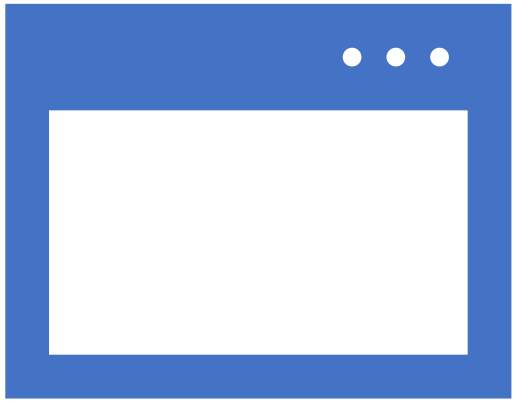
Prompting you to download something.

Headlines that are ambiguous and sensational that encourage you to click to read more are called clickbait.

Online shop or pay bills from your home connection.

# Understanding Browser Tracking

- Whenever you're online, the sites you visit and the stuff you click on all leave a little trail. Websites use things called cookies to remember what you've been up to in your web browser. Also, they might keep an eye on your browsing through your user accounts. It's not usually a big danger to your online safety, but it's good to know how your info gets tracked and used.
  - YouTube and Netflix collect information on the videos you watch, which helps them suggest more videos you might like.
  - Online stores like Amazon and Walmart keep records of different items you view and purchase, which helps them suggest other products.
- Cookies remember details about the websites you check out and the stuff you click on while surfing. If you don't have an account on a site, this info usually gets stored in a cookie right in your web browser. For instance, let's say you visit a news site. It might use cookies to remember if you've been there before and what stories you liked, so it can recommend similar one's next time you quickly visit.



# Networks

- If you're using Wi-Fi at home, it's important to keep it safe from sneaky folks who might try to snoop on your stuff. Setting up Wi-Fi security might seem tricky, but don't worry! If you're not sure what to do, you can always ask your internet provider for help. Here are some easy tips to keep your Wi-Fi safe:
  - Keep your Wi-Fi signal just strong enough for your house, so it doesn't reach too far.
  - Hide your Wi-Fi name from other people nearby.
  - Choose a strong password or phrase that's easy for you to remember but hard for others to guess.
  - Use MAC address filtering to stop any unwanted devices from connecting to your Wi-Fi.
  - Make sure your Wi-Fi uses WPA or WPA2 for security.
  - If you're using WEP, try to make sure it's got the strongest encryption possible.

# Resources and Support

- Tech Life Unity
  - https://www.techlifeunity.com/a-to-z-topics
- Be Internet Awesome for Kids by Google
  - https://beinternetawesome.withgoogle.com/en_us
- Older Adults Technology Services from AARP
  - https://oats.org/digital-equity/
  - 888-713-3495
    - Hotline hours: Mon-Fri, 7:00am-6:00pm MT / Sat, 7:00am-12:00pm MT
- Goodwill Community Foundation
  - https://edu.gcfglobal.org/en/

# Conclusion

Create strong Passwords

Prioritize your personal health and wellbeing by thinking before you click.

Reach out to a trusted source if you need support.