Orleans Digital Literacy Initiative

Online Safety

This module will take a general look at online safety. It will cover creating strong passwords, using a password manager, sharing accounts, phishing, and how to identify online scams.

Cybersecurity Terms

→ Cybersecurity is the practice of keeping our digital lives and our computers safe and secure.

Malware - Software that is meant to do harm to a computer system, whether it be to take information, hold ransom, disable, or something else.

Virus - A specific type of computer malware that self-replicates and spreads to other computers.

Network - The connection of computer devices generally relating to a home or business.

Internet - The broader connection of computers across networks.

Antivirus - Software that scans a device or a network to detect security threats, alert you, and neutralize malicious code.

Authenticator - A method of how a user can prove his/her identity to a system. It can be a password, a fingerprint, a face scan.

Virtual Private Network (VPN) - Technology that extends a private network and all its encryption, security, and functionality across a public network. With it, users can send and receive messages as if they were connected to a private network.

Online Data

When posting or giving information or data online, it is important to be aware of what you are sharing and the potential for misuse.

You should always be aware of the information and data when you are posting to social media platforms, shopping online, signing up for accounts, and any time you enter your Personally Identifiable Information (PII) on a device.

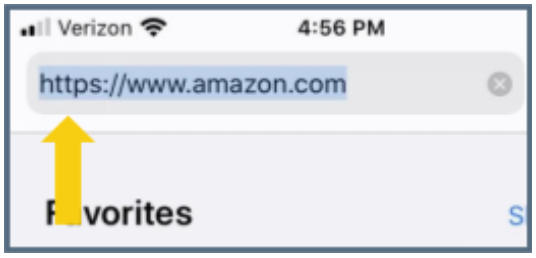
Personally Identifying Information (PII) is any information that can be used to figure out who you are and potentially steal your identity. This includes your name, birthday, address, social security number, credit card information, and more.

- ★ Make sure that files with PII are stored in places that your employer or organization wants them to be stored.
- ★ Make sure that files downloaded to your computer are erased to avoid being opened by individuals that should not be accessing them.
- ★ Make sure any files or images you store on a mobile device are saved in the correct places and are removed from any place that is unsecure, in case of loss or theft of the device.

HTTP vs. HTTPS

Is this website secure?

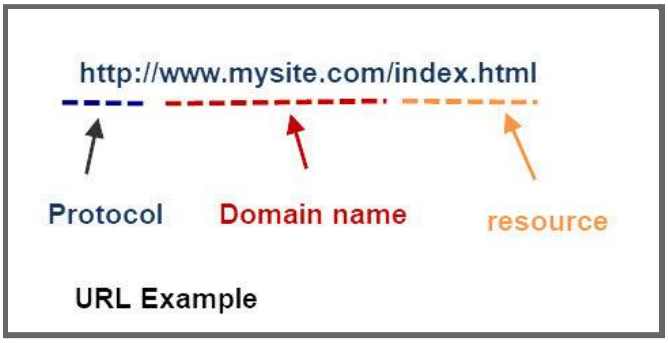
There are two protocols for how information from your browser gets to a website and how information gets from the website to your browser. **HTTP** stands for HyperText Transfer Protocol, and **HTTPS** stands for HyperText Transfer Protocol Secure.



Amazon.com is using HTTPS

The main difference is that HTTPS is secure (encrypted) and HTTP is not.

- ★ Someone who maliciously intercepts our data when we use HTTP can see or read what we have sent
- ★ Someone who maliciously intercepts our data when we use HTTPS cannot see or read what we have sent



The URL structure of an http: hosted website

You should never send any PII over HTTP. Only send it over HTTPS.

Orleans Digital Literacy Initiative

Never post PII to a shared drive like Google Drive or to a shared calendar space. PII should be shared only with those who need to know it.

Some ways to check if a website is legitimate can be:

- ★ Who is the author of the source?
- ★ Where was the source published?
- ★ What information does the source include?
- ★ Why did the author create the source?

Scams & Phishing

What is a Scam?

A scam is a term used to describe any fraudulent scheme that takes money or other goods from an unsuspecting person. Online scams have become very prevalent. While they used to be pretty obvious, they have become more sophisticated in recent years. Scams can be simple or more complex. They are similar in nature to phone scams. They can be found in email, websites, and on social media. Remember: If something seems too good to be true, it probably is!

Types of Scams

A **Donation Scam** is where a scammer pretends to be a charity so you will "donate" to it. However, you actually end up just giving the scammer your money.

Catfishing is when a scammer crafts a fake persona or identity in order to trick someone into giving them something they want.

A **419 or "Nigerian Letter" Scam** is a scam where the scammer asks to be sent an amount of money to cover some cost in order to award the recipient of the letter/email with a large sum of money.

An **Online Survey Scam** is a scam where a scammer offers usually either money or some good prize, like an iPad, but you have to fill out a survey. These surveys will often ask personal information, especially those found on security questions, to try and identify you and gain access to your accounts

Scammers will use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, credit cards, or other accounts. Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.

Tactics used in Phishing Scams:

- ★ Scammers say they have noticed some suspicious activity or log-in attempts
- ★ Ask you to confirm your personal information
- ★ Ask you to click on a link to make a payment
- ★ Offer a coupon for free stuff

Password Safety

Secure passwords go a long way toward keeping you safe online.

Password Do's:

Do create a unique password for each account you use.
Do use a random mix of numbers, letters, and symbols.
Do use a password manager to help you keep track of your unique passwords.
Do only submit your passwords to appropriate (secure) sites.

Password Don'ts:

Do not use common phrases or personal information (i.e. a pet's name)
Do not write your passwords down.
Do not share your passwords.
Do not make short passwords.
Do not make a password that is easy to guess.
Do not keep the same password for a long time.
Do not store your password where it can be easily found.

Examples of Good & Bad Passwords

Examples of Bad Passwords	Examples of Good Passwords
Password	@H76cxgV90$$jKTsk
John2021	IegtDL2021!
03-21-1990	P3aS0up4me
Wizard22	nwso^d-scr23ap(hk3dh

Safely Storing Passwords with Password Managers

A **password manager** securely stores your passwords and logins as well as other information that you need to keep private, but access easily. Some popular password managers are LastPass, 1Password, or Dashlane. Password managers have apps that you can download onto your computer or mobile device and web-based applications that you can access from any device. They have a variety of free or paid plans that you can tailor to your needs.

It is best to avoid sharing login credentials whenever possible. However, sometimes sharing an account within your family is unavoidable. This is where password managers can be helpful. Some allow you to put multiple users on a family or business account which allows you to securely share passwords with a trusted individual. Others allow you to invite a guest to access only the passwords you want to trust them with. Either way, make sure that you trust this individual and there is no alternative to sharing the same credentials.

LastPass

1Password

Dashlane

Orleans Digital Literacy Initiative

Multi-factor Authentication

Multi-factor authentication is when several factors are required to perform a successful identity verification. Once you have correctly entered your password into a website, the system will then send you a code via text message or ask that you retrieve a code from your Authenticator app. You will then be required to enter this code to finish signing into your account.

Multi-factor authentication, also known as two-factor authentication, adds an extra layer of protection. Multi-factor authentication can give higher security levels when combined with lower quality methods (e.g. a simple password) as people with malicious intent would have to not only know your password, but also have access to your device to get the code from the multi-factor authenticator app or text message. Multi-factor authentication is ideal where security is more important than ease of access. Note: When given the option of a password or biometry, biometry is always stronger than a very-hard-to-guess password.

Examples of biometry on a mobile device are fingerprint scans or facial recognition.

Anti-Malware

Anti-malware software is also known as anti-virus software. It is a type of software that helps prevent malware on a computer. Anti-malware software can scan your computer or scan downloaded files to find malware. It is important to note that anti-malware software does not prevent all malware so it is important to still use other safe practices.

Windows Defender is a good anti-malware software that comes pre-installed on Windows computers.

Windows Defender logo

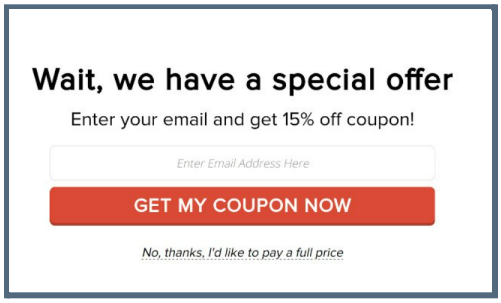
How to Protect Yourself from Malware

One of the best and easiest things you can do is keep your software applications up-to-date with the latest versions of software updates provided by the software maker. You can set your applications to auto-update to receive the most up to date versions of your software applications. Another action you can take is not to use websites, applications, or tools that are not trustworthy. Always make sure you do not disable any anti-malware settings. Finally, do regular scans with your computer's anti-malware software.

Pop-Ups and Ads

When you are using web browsers, you have to watch out for pop-ups and ads.

Pop-ups are windows (or text/graphic squares) that block you from viewing a website or something else until you close them. **Ads,** or advertisements, are things trying to get you to do something such as clicking and going to a shopping website. They can be malicious by either forcing you to click on something, collect information from you, or scam you.



Example of a popup advertisement

It is important to note that not all pop-ups and ads are malicious. The way to tell if a pop-up or ad is malicious is going to come down to the content. For example, a website asking for your email address for a newsletter may not be malicious. On the other hand, a pop-up saying "You won a free iPad!" or "Your computer has 20 viruses, clean now!" may be malicious. Important things to always remember are: Does it fit into the website? Is it over the top or too good to be true? **Is this something I need to click on?**

Social Media Safety

Social Media Tip: There is a social media trend that is going around that creates a fun character name using things like your birth month, middle name, and the street where you live? Beware of this type of request to post/share: Your post could be used to collect information about you!
Best to sit this one out.

Tips when using social media...

- ★ Be cautious of sharing too much
- ★ Adjust your privacy settings
- ★ Verify who you are connecting with
- ★ Do not share personal details
- ★ Remember what goes online, stays online
- ★ Keep passwords strong

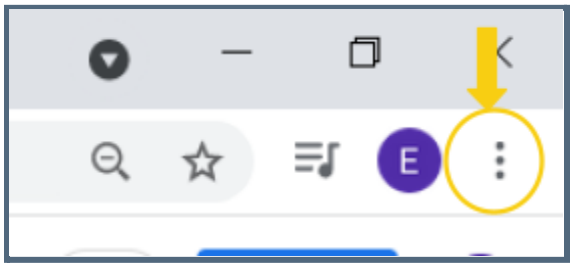
Downloading Files

When downloading files these are important things to always remember:

- ★ Make sure you trust the website that you are downloading from
- ★ Make sure you know what you are downloading
- ★ Make sure you are clicking on the right link

Incognito Browsing

When browsing the internet there are certain things that are stored on your computer such as **cookies**, which are pieces of information that can be used to track information from your internet browsing, and browsing **history**, which is a record of the websites you have visited. If you wish to block these you can use your browser's **incognito** mode. You can access your browser's incognito mode by clicking in the menu usually found in the top right corner of your browser and selecting "New incognito Window" or "New Private Window."



First step to opening a browser in incognito mode is to click the three dots on the right side of your browser.

Next step is to choose "New Incognito window," which will open a new incognito window

Using an incognito window means that you will not remain signed into any of your accounts, have targeted ads, or have the session show up in your browser history. This is a good way to keep your browsing sessions more secure on a shared computer.

Digital Hygiene Summary Reference

- ★ Ensure your computers have up-to-date software
- ★ Use two-factor authentication (2FA)
- ★ Be cautious of clicking on links or opening attachments in emails
- ★ Implement privacy settings on social media accounts
- ★ Install Anti-Malware Software
- ★ Use complex passwords
- ★ Do not use "free" non-secure WiFi
- ★ Make sure that the websites you visit use HTTPS
- ★ Do not share your devices
- ★ Dispose of electronic devices securely

Orleans Digital Literacy Initiative

A piece of general online safety advice.

Trust your gut. If a website doesn't give you a good feeling, don't submit any sensitive information on it.