How to Guide: Internet Safety, Ethics, and Identifying Credible Sources

What is Internet Safety?

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet—at home, at school, at work, or on our mobile devices—we make decisions that affect our cybersecurity. Internet Safety or Cyber Safety is the art of utilizing the Internet in a safe and secure way to protect your information and reduce risks to others. Emerging cyber threats require engagement from the entire American community to create a safer cyber environment—from government and law enforcement to the private sector and, most importantly, members of the public.

Internet safety covers many things including:

- Impersonation
- Malware
- Passwords

Alabama A&M University
FAMU Florida A&M University Cooperative Extension College of Agriculture and Food Sciences
Fort Valley State University Empower the Possible.
North Carolina Agricultural and Technical State University
Prairie View A&M University
Purdue University Center for Regional Development
SRDC Southern Rural Development Center

Impersonation

Impersonation is one of the most common forms of internet safety on a personal level. Online impersonation refers to creating an online presence or profile using a likeness that is not your own, or that of someone else.

Impersonation	Definition
Phishing	Phishing is the fraudulent practice of sending emails messages purporting to be from reputable companies to trick individuals to reveal personal information, such as passwords and credit card numbers. Phishing looks very realistic but has several red flags such as a generic greeting, request for private information, and an invitation to click on a provided link.
Spear Phishing	Spear Phishing is phishing method that targets specific individuals or groups within an organization to trick users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss.
Smishing	Smishing is the fraudulent practice of sending text messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords or credit card numbers.
Vishing	Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.
Whaling	Whaling is when someone masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes. The term whaling stems from the size of the attacks, and the whales are thought to be picked based on their authority within a company such as a senior executes, CEO, CFO, government officials, etc.

Impersonation Activity - https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/phishing

Malware

Malware is software that intentionally inflicts damage on its users who typically have no idea that they are running it.

Types of Malware	**How it is Spread**
Computer Virus	replicate by inserting their own code into computer systems
Worms	replicate themselves without the need for hosts to spread
Trojans	disguised as non-malicious software or hidden within a legitimate, non-malicious application
Ransomware	demands that a ransom be paid in exchange for the infected party not suffering some harm
Scareware	scares people into taking some action
Spyware	surreptitiously, and without permission, collects information from a device.

Avoiding Malware

- Install and update security software and use a firewall.
- Read the screen before you install new software
- Get only well-known software – directly from the source
- Pay attention to security warnings
- Do not click on provided links – go to site directly
- Scan external devices before using them

Malware Activity - https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware

Passwords

A password is a secret word or phrase that must be used to gain admission to something.

Password Strategy

- Prioritize password **length**
- Include a **combination** of letters, numbers, and symbols
- Avoid using real **words**
- Never use **personal** information
- **Never repeat** passwords
- **Multi-factor** authentication
    - Something you **have**
    - Something you **are**

Top Ten Passwords

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 12345
6. Qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Password Activity - If participants have smart devices, have them go to the website and enter passwords, (not their real ones), to see how secure they are. https://www.security.org/how-secure-is-my-password

Digital Estate Planning

Now that we have gone through password security, what happens when someone needs to get access to your electronic devices after you pass.

- **Sharing Passwords**
- **List Digital Assets**
- **Legacy Accounts**
    - Facebook Legacy Account https://www.facebook.com/help/1568013990080948
    - Google Inactive Account Manager https://support.google.com/accounts/answer/3036546?hl=en
    - Apple Legacy Account https://support.apple.com/en-ca/102631

Activity: Have participants create a draft digital estate guide including social media accounts, hardware such as computer, tablets, phones, etc., and actions on what to take upon death such as keep open, delete, etc.

Digital Estate Planning Example		
	Username/Password	**Action**
Hardware		
Social Media Account		

Identifying Credible Sources

CRAAP Test	
Currency	The timeliness of the information
Relevancy	The importance of the information for your needs
Authority	The source of the information
Accuracy	The reliability, truthfulness, and correctness of the content.
Purpose	The reason the information exists
Other Sources of Evaluation	
RADAR	Rationale, Authority, Date, Accuracy, Relevance
SIFT	Stop; Investigate the source; Find better coverage; Trace claims, quotes, and media to the original context
5Ws	Who, What, When, Where, Why

CRAAP Test Activity

Do a Google search for a topic of your choice. Using what you learned about the CRAAP test, find two websites, one that you would be able to use as a source and one that you would not use as a reliable source. Fill in the chart for each website.

- **GOOD WEBSITE**: copy and paste the URL (usually starts with WWW or HTTP)

Rate each of the categories in CRAAP for this website. 1=bad, 2=ok, 3=good. Then give a reason why you gave it that rating.

	Rating	Reason
Currency		
Relevance		
Accuracy		
Authority		
Purpose		

- **BAD (or not as good) WEBSITE:** copy and paste the URL (usually starts with WWW or HTTP)

Rate each of the categories in CRAAP for this website. 1=bad, 2=ok, 3=good. Then give a reason why you gave it that rating.

	Rating	Reason
Currency		
Relevance		
Accuracy		
Authority		
Purpose		

Digital Ethics

Digital ethics is the acceptable behavior standards to be followed by digital users while using the internet. They help digital citizens stay safe online by setting up a set of moral principles that govern the usage of Computers and Internet.

Question	Response
How should people treat each other online?	
Should a person download media without paying for it?	
How should a person respond when he or she realizes someone else is being bullied?	
Can internet users post whatever they want online?	
What about spreading false information or pretending they are someone else?	

This project was funded by USDA NIFA award # 2022-68006-36496. The material is based upon work supported by the National Institute of Food and Agriculture, U.S. Department of Agriculture. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of the U.S. Department of Agriculture.

December 2023