INTRO TO INTERNET PRIVACY & SECURITY
OBJECTIVES

- Increase knowledge and awareness of internet risks
- Become familiar with lingo
- Gain confidence that internet safety and privacy is manageable
- Become familiar with social media privacy settings
STRIKE A BALANCE

Digital Age Advantages

Risk Awareness
RISKS ARE HIGHLY INTERCONNECTED

Falling victim to one risk may make you more vulnerable to another...

.. But protecting yourself from each risk makes you less vulnerable to every other risk.
TODAY’S TOPICS

- Malware
- Phishing
- Account hacking
- Scams and frauds
- Social Media and Internet Privacy
Definition: Software that gets installed on your computer without your consent.

Types: Viruses, spyware, adware, Trojan horses.

Potential damage: cause your computer to crash or work very slowly or not work at all, pass on viruses to other computers, allows strangers to monitor your computer activity.

How to detect malware: slow computer, computer won’t shut down or restart, pop-up ads, browser opens web pages you didn’t choose.
PROTECT YOURSELF FROM MALWARE

**DO NOT**
- Click on links in emails (even those that appear to be from friends).
- Open attachments in emails (even those that appear to be from friends).
- Click on pop-ups that appear – no matter how interesting or important they appear to be, e.g. “your computer has been infected!”

**DO**
- Keep your operating system up-to-date.
- Keep your internet security software up-to-date and activated (so that it regularly scans your computer).
- Be aware of what is ‘normal’ for your computer – how fast it runs, how websites look.
If you have active anti-virus software on your computer, that software did NOT spot and stop the malware. Make sure your software is up-to-date.

Malware removal tool can be found in our Internet Safety Guide on our website (eResources→Research Guides→Internet)
Malware
Phishing
Account hacking
Scams and frauds
Social Media and Internet Privacy
PHISHING

- An email or phone call purporting to be from a company.
- Attempt to get you to enter or provide account or other personal information.
- NO legitimate company will send you an email asking you for your username and password.
- NO legitimate company will call you and ask you for your information.
- To be safe, call the company yourself or go directly to the website on your computer.
Dear HSBC Customer,

Your Internet Banking security number was entered incorrectly more than 3 times. For the protection of your account we have suspended access to it. To restore access please Log on correctly.

Previous notifications have been sent.

Thank you for choosing HSBC Bank.
Copyright HSBC INC 2010. All rights reserved.
PHISHING CHARACTERISTICS

- Bad spelling or grammar.
- Incorrect information.
- Sender email address does not match purported website (e.g., amazon.org, amazon-security.com).
- Sense of urgency.
- Often refers to internet security or invoices, orders, or payments.
## CHECK YOUR SPAM FOLDER

Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

<table>
<thead>
<tr>
<th>Sender</th>
<th>Message Details</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derick Curry</td>
<td>Payment Confirmation - Dear Valued Customer, Your Invoice appears below. Please remit payment at your earliest convenience.</td>
<td>Mar 2</td>
</tr>
<tr>
<td>Weldon Pardeus</td>
<td>Unpaid invoice # 002319167 - Dear Client, According to the reconciliation of the Department of Finance there are the areas</td>
<td>Mar 1</td>
</tr>
<tr>
<td>Penny Batu</td>
<td>Invoice #33215558/15 - Dear custumer, You are receiving this informational letter because of the fact that you have a debt</td>
<td>Feb 29</td>
</tr>
<tr>
<td>Facebook</td>
<td>You have more friends on Facebook than you think - The fastest way to find all of your friends on Facebook is importing your email contacts. Once you</td>
<td>Feb 29</td>
</tr>
<tr>
<td>Facebook</td>
<td>You have more friends on Facebook than you think - The fastest way to find all of your friends on Facebook is importing your email contacts. Once you</td>
<td>Feb 25</td>
</tr>
<tr>
<td>Bertha Garcia</td>
<td>Invoice 85413452 - Dear akaga, Please review the attached copy of your Invoice (number: IN85413452) for an amount of</td>
<td>Feb 24</td>
</tr>
<tr>
<td>Matt Alleman</td>
<td>Central phones - The phones at central are having issues calling out. It should be fixed soon but I apologize for the</td>
<td>Feb 23</td>
</tr>
</tbody>
</table>
TODAY’S TOPICS

- Malware – including viruses, spyware
- Phishing
- Account hacking
- Scams and frauds
- Social Media and Internet Privacy
ACCOUNT HACKING

- Definition: Somebody accesses your electronic account without your permission.
- Types: Email, social media, websites.
- Potential damage: identity theft, professional or personal reputation.
- How to detect: your account username and password don’t work, you are locked out of your account, your friends tell you they received a strange email from you, your Facebook timeline includes things you didn’t post.
WAYS YOU CAN GET HACKED

- Brute force: someone has your email address and guesses at the password.
- Man-in-the-middle: you are on a public wi-fi network or on an unencrypted home wi-fi network and not using an encrypted site.
- Trojan horse: you have downloaded and installed software that gives hackers access to your keystrokes.
- Phishing: you log in to or provide your account information to a look-alike website or company communication.
STRONG PASSWORDS

- Use a combination of lower-case and upper-case letters, numbers, and special characters (e.g., /, @, #).
- For your own benefit, devise a password that is easy for you to remember (but hard for others to figure out).
- Substitute numbers for letters, e.g. GR8T for ‘great’
- Substitute special characters for letters, e.g. f!sh!ng
- At least 8 characters long.
- Do NOT use street address, pets’ names, children’s names, birthdates, or similar information.
# YOU HAVE A SECURE CONNECTION IF…

<table>
<thead>
<tr>
<th>Browser</th>
<th>Security Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Green padlock image to the left of the website name and website name begins with https://</td>
</tr>
<tr>
<td></td>
<td><img src="https://ssa.gov" alt="Social Security Administration (US) - https://ssa.gov" /></td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Green padlock image to the left of the website name and website name begins with https://</td>
</tr>
<tr>
<td></td>
<td><img src="https://twitter.com/" alt="https://twitter.com/" /></td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Padlock image to the right side of the website name and website name begins with https://.</td>
</tr>
<tr>
<td></td>
<td><img src="https://www.wellsfargo.com" alt="https://www.wellsfargo.com" /></td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Padlock image to the left of the website name</td>
</tr>
<tr>
<td></td>
<td><img src="https://facebook.com" alt="facebook.com" /></td>
</tr>
</tbody>
</table>
A SECURE CONNECTION ...

- ...is very important when shopping online, accessing online bank accounts, etc.
- ...means that your information is encrypted and sent to the recipient, then decrypted at the recipient’s end. Information sent to you by the recipient is decrypted, then sent, and decrypted for your use.
- ...does NOT mean that you are connected to a legitimate business or organization. For example, if you click on a link in a phishing email that looks like an Amazon email, you may find yourself in a website with a secure connection, but it will not necessarily be the Amazon website.
Use encryption and password protection options on wireless router in home network

Be wary of accessing sensitive information when using public wi-fi networks. Make sure encryption is on (https).

Be aware of how you log in to any accounts when on a public computer – don’t turn on option to “keep me signed in”. Make sure to always log off.
TODAY’S TOPICS

- Malware – including viruses, spyware
- Phishing
- Account hacking
- Scams and frauds
- Social Media and Internet Privacy
SCAMS AND FRAUDS

- Definition: dishonest way to make money by deceiving people (scam, Merriam-Webster) via the internet.
- Types: Nigerian, traveler in distress, sweepstakes winner.
- Potential damage: financial loss.
- How to detect scams and frauds: too good to be true, flattery, sense of urgency, requests for account numbers or personal information, requires cash up-front.
TODAY’S TOPICS

- Malware – including viruses, spyware
- Phishing
- Account hacking
- Scams and frauds
- Social Media and Internet Privacy
Social media sites like Facebook, Twitter, and Instagram are all about sharing.

You can share things publicly, with groups of people, or with individuals. Companies like Facebook also have access to some information about what you share.

It's important to be aware of who you're sharing things with and WHAT you're sharing. Sharing a photo of yourself on vacation to your friends and family is one thing—but if you share it publicly, you've just announced you're away from your home, making you potentially vulnerable to a crime.

Many websites allow you to send private messages to individuals, or limit posts to particular groups.

Keep in mind that social networking companies have access to the information you post. Look for a privacy policy on each site to see how your information is being used.
Before sharing information online, ask yourself these questions:

- Do you want everyone to be able to see this?
- If not, who do you want to limit it to?
- Will it come up if you search for your name on Google?
- Will employers or strangers be able to find it?

Once something is shared online, it can be very difficult to completely erase if you change your mind later.

adapted from digitallearn.org
When searching the web, your searches are often saved on the computer you’re using. The search engine company can also see information about what you’re searching for.

Web browsers have settings you can apply to control the information that is tracked and saved, e.g. passwords, history, cookies (more on cookies in a minute).

Anytime you visit a website, information is collected, including your geographic location, the links you click on, and other information about your web browser, computer, or other device you’re using (cookies).

The information generally doesn’t identify you as an individual, but gives the website owner helping information about demographics and technologies their visitors use.

Some websites collect more specialized information—they may scan for keywords you use, and use those words to show tailored advertisements to you (cookies).

adapted from digitallearn.org
More on Cookies...

Every time you visit a site, a small text file is downloaded to your computer that makes browsing that site easier. Cookies do things like save passwords so you don’t have to enter them every time, remember your search history and help webpages you visit frequently load faster and provide you with tailored information. If you’ve ever gone to Google and noticed something you searched for yesterday on Amazon showing up in the sidebar, these are cookies at play.

If you block cookies, some websites may not load correctly, or allow you to sign in, or you might see a message that cookies are required to use that site.

To keep your searches private, use your browsers private browsing option—this will keep the company from tracking your searches and won’t save your search history.
SAFE SURFING

- Be wary of offers that are too good to be true
- Be wary of security or other ‘scary’ warnings that appear unexpectedly
- Be aware of what the websites you use the most look like and how they operate
- Be aware of how your computer normally operates (speed, desktop appearance, rebooting)
- Be aware the privacy settings available to you on social media and in your web browser
- Most of all,

THINK BEFORE YOU CLICK
INTERNET SAFETY RESEARCH GUIDE

All the info included here plus what to do if your computer gets compromised, or if you get hacked, or have your identity stolen.

- Library website (https://mesacountylibraries.org)
  - eResources
    - Research guides
      - Internet safety