IT 101

TOPICS:

- Phishing / Cyber Security
- Passwords
- Safe Computing
- Copyright
- Acceptable Use
- Updates
- Civility in CyberSpace

PHISHING / CYBER SECURITY

Email Impersonation Attacks Rely on Spoofing

Phishing

Definition: to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks like it is from a legitimate organization, usually a financial institution, but contains a link to a fake Web site that replicates the real one.

In general, most entities (e.g. banks, health care organizations, academic institutions) will not initiate electronic communications that request your account number, social security number, credit card number, insurance ID, etc. Do not give out personal or sensitive information in electronic mail messages.
Please DO NOT forward emails you suspect as Phishing.
Rather use the "Phish Alert Tool" in your Outlook ribbon.

The Latest in Phishing: January 2020
Proofpoint State of the Phish - 2020 - (SCmagazine.com)
“Spear Phishing” is a new approach that relies on emails that appear to be from a source you trust (IT Department, IT Help Desk, your Employer, etc.).

What To Do:

1. Check where the email came from. Generally someone’s legitimate email address was spammed to send this email to everyone. Be suspicious of email addresses you do not recognize or simply does not look right.
2. Grammatical and punctuation errors as well as low-resolution logos are big warning signs.
3. Hover over clickable links in the email and a box will appear with the address they want you to click on - another warning sign - do not click on it.
4. The IT Department will never ask you to verify your account, disrupt or lock your account if you don’t act immediately, suspend your email service or ask for you to give us your password.
5. Never share your password and be sure to change it often.
6. Call the It Help Desk if you have any questions or are unsure about an email you received at 717-871-7777.

Choosing a Password

Creating a secure password is vital for successfully managing your life on the Internet.

See the links below to help you create a secure and easy to remember password(s):

- Creating Strong Passwords
- The Importance of Using Strong Passwords
- Cnet.com - The guide to password security (and why you should care)
In an effort to enhance security and to protect your account, please change your password. Visit millersville.edu/login today!

LEAKS MAKE US WEAK!

Keep our information secure. Use a strong, unique password for every login!
In an effort to enhance **security** and to **protect** your account, please change your **password**.

My password mixes **uPpEr** and **loWer case**, **L3+tEr$**, **Num&3rS** and **$yMb0L$**.

Visit [millersville.edu/logins today](http://millersville.edu/logins)!
SAFE COMPUTING

Computer Virus, Malware, Adware, Spyware, Worms, Trojans...

- **Virus**: is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- **Malware**: software programs designed to damage or do other unwanted actions on a computer system.
- **Adware**: is free software that is supported by advertisements, such as toolbars that work in conjunction with your Web browser. Most are safe to use, but some can serve as spyware gathering information from your hard drive, the Web sites you visit, or your keystrokes. Be careful what adware you install on your computer.
- **Spyware**: is software that "spies" on your computer. It can capture information like Web browsing habits, email messages, usernames and passwords and credit card information.
- **Worms**: is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- **Trojans**: at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.

Do you really need antivirus software? ([ZDNet.com](http://www.zdnet.com)) - Yes! A very good resource for all you wanted to know about the benefits of antivirus software and were afraid to ask. Just how dangerous is it out there? You’d be surprised. See the essential steps you need to take to keep your Windows PC safe.

Some recommended antivirus software:

- Windows Defender Antivirus
- SUPERAntiSpyware
- Malwarebytes Anti-Malware
- AVAST

How did my computer get infected?

1. Your computer does not have antivirus software installed.
2. Your antivirus software does not have the most up-to-date virus definitions.
3. Your PC is behind in its Windows Updates.
4. You clicked on a link or attachment in an email without questioning the source. If the email sender is unknown, delete immediately. Be suspicious of emails from friends - could be spam - always ask to be sure. It is always best to delete suspect emails and have them sent again if necessary.
5. The administrator password on your Windows PC is blank.
6. You clicked on the flashing message that popped up on your computer telling you "Your computer is infected with viruses - click here to clean your computer" and you've unwittingly opened an executable file that might bring your PC to its knees. Sometimes also clicking the "cancel" button will yield the same results. Always try the "X" to close. If it will not let you click the "X", close the program and/or shut off your PC.
7. You clicked on a popup that looks like a Windows message or alert. Many of them look very convincing and when you click on them they take you to another website to try to get you to download software. You can check to see if it’s a proper alert by right-clicking on the window. If there is a menu that comes up saying “Add to Favorites” - you know it is a fake.
8. You downloaded software from the Internet that was infected. To check the validity of software downloads see: Norton Safe Web.
9. You opened an infected file from an external drive. Be sure to run virus scans on any flash or external drives.
10. You did everything right and it still happened. Unfortunately that is very true, however you can be prepared and practice safe computing.

COPYRIGHT

Copyright Infringement

Downloading or distributing whole copies of copyrighted material for personal use or entertainment without explicit permissions from the copyright owner is against the law. Copyright law applies to materials such as music, movies, games, or software.

How the University Addresses Allegations of Violation of Copyright involving On-Line Materials
ACCEPTABLE USE

Acceptable Use Policy

Millersville University's expectation of responsible, considerate, and ethical behavior extends to cover the use of campus microcomputers and workstations, departmental computer facilities, general-use computer, campus network resources, video conferencing, fax, telephone, cable TV, and networks throughout the world to which the University provides computer access. Use of University resources must comply with State and Federal law and University policies.

Policy for Responsible Use

UPDATES

Keep Your Computer Up-To-Date

Keeping your computer (Windows PC or Mac) current with updates for your operating system and software is essential to a healthy computer. Both Windows PC's and Mac computers can be set to automatically update.

- Windows PC’s
- Mac Computers

CIVILITY

Civility in Cyberspace - Be Cyber Savvy

Avoid the Impulse. Remember, what you do reflects on you.

If you engage in an impulsive negative act that results in posting or sending material in digital format, this material can become widely disseminated and possibly permanently available. This could harm your reputation, friendships, and opportunities; place you at risk; or cause harm to others. Engage in effective problem solving and positive decision making before posting or sending anything. Be a helpful ally if you see someone is at risk or is being harmed.

Read With Your Eyes Open. Assess the credibility of information.

Anyone can post or send anything online and there is no guarantee that what has been posted or sent is accurate. Individuals, organizations, and companies may use sophisticated techniques to seek to influence your attitudes and behavior. Carefully assess the credibility of all information accessed on websites or received in messages and the trustworthiness of people in which you interact.


While use of digital technologies can be fun and allow you to connect with your friends, excessive use of digital technologies can be unhealthy. Ensure your use of digital technologies does not interfere with other activities that will make your life happy and successful.

Think Before You Post. Protect your reputation and respect others.

Other people will judge your character and decision making based on the material you post and send. This can affect your reputation, friendships, and opportunities positively or negatively. You can hurt others if you post or send material that reveals their personal information. Be careful whenever posting or sending material in digital format. Respect the rights and privacy of others.

Connect Safely. Interact safely with others online.

You will interact with many different people online. Most are safe and trustworthy, but some may not be. It is easier for people to be deceitful and manipulative online. Be careful when you interact with people online. Only let people you know, or those whom your good friends know, have access to your personal profile. If you want to meet in person with someone you have gotten to know online, make a safe meeting plan and bring along friends.

Keep Yourself Secure. Implement security and avoid scams.
Digital technologies can be corrupted with malware, which often is used to commit identity theft. Criminals use the Internet to commit a variety of scams. Ensure your computer security is maintained and your activities do not increase your risk. Watch out for scams—offers that are too good to be true or threaten loss if you do not share personal information.

Abide by the Terms. Act in accord with policies, terms, and laws.

Your online activities are governed by laws, use policies of the organization that provides your access, and the terms of use of the websites or services. These laws, policies, and terms ensure that user's activities do not cause harm to others or to the technical system. Follow the standards to protect the rights of everyone.

Stay Out of the Garbage. Avoid objectionable and illegal material.

People distribute materials online that are harmful to others, including pornographic material. You could accidentally access this material. Accessing or distributing child pornography is a serious crime. Use safe surfing techniques to avoid accidentally accessing this material. Know how to effectively respond if such material is accidentally accessed. Don't access or distribute child pornography.

Don't Sell Yourself. Disclose and consume wisely.

The financial model of the Internet involves providing access to free content and services in exchange for market profiling and advertising. Sites and apps track your postings and activities to create a market profile that guides the advertisements you will see. Social networking sites encourage friends to send advertisements to their friends. You can find helpful information about companies and their products or services online. Make a personal decision about how much personal information you want to share with sites and apps. Use the Internet to research companies, products, and services prior to making purchases.

Protect Your Face and Friends. Be savvy and civil when networking.

Social networking sites are fun places to post information and connect with friends but present risks that involve posting inappropriate material or engaging in unsafe interactions with others. These sites encourage users to share personal information and have many friends so they and their advertisers can obtain market profile information and use friendship connections to encourage purchasing. The terms of use prohibit hurtful actions. Protect your privacy by limiting access to your profile to those you have friended. Protect your reputation and respect others when you post. Friend only people whom you or a trusted friend know in person. Report abuse.

Cyberdate Safely. Avoid exploitation and abusive relationships.

Watch out for fantasy relationships. Recognize that forming close personal relationships primarily through digital technologies can lead to unrealistic understandings and expectations. Proceed with caution when forming a relationship digitally. Avoid exploitation. Do not allow a partner to abuse you. An abusive partner may try to use digital technologies to control you by constantly texting and controlling your digital communications with others. Do not allow a partner to seek to control you in this manner.
Help Desk

Help Desk Contact Info
Location: Bard Hall
Phone: 717-871-7777
Email: help@millersville.edu
Classroom Hotline: 717-871-7280
After Hours D2L Help: 877-325-7778

Hours:
Call Center
- Fall/Spring Semesters:
  - M-TH 8AM - 7PM EST, F 8AM - 5PM EST
- Summer Sessions:
  - M-F 8AM - 4PM EST

Walk-in TAC
- M 9-11AM, 12-7PM
- T 11AM-4PM
- W 9-10:30AM, 1-7PM
- TH 9AM-5PM
- F 9-11AM, 1-4PM

By Appointment - book an appointment

Technical Assistance Center - Bard Hall