

TECH *bits*

CONTACT:

Sheryl Priestster, Technology Trainer

Phone: (239) 377.0417

Email: priess@collierschools.com

"Interesting Tidbits about Technology"



DID *you* KNOW?

The purpose of cyber security awareness month is simply to focus attention on keeping you, your computer, your data, and your identity safer. Here are a few steps you can take to not only participate in National Cyber Security Awareness Month, but also enhance cyber security 365 days a year:

Be defensive with sensitive information

- Avoid sharing sensitive/personal data in email, instant messages (IM), or text messages.
- Check a webpage for encryption indicators (like "https" in the address and a closed padlock). Secure websites start with https. Always confirm if website URL is correct. It is always good idea to type the website url directly in the browser and avoid following link from email.
- Save banking, shopping, and other financial transactions for your home computer. District computer systems are for "Business Use Only".

Create varied & strong passwords or phrases

- Aim for length, complexity, and variation.
- Use capital and lowercase letters, numbers, and symbols; keep them secret.

Watch out for scams

- Be wary of email messages with urgent requests for personal information.
- Be on the lookout for misspellings and grammatical errors or deals or prizes that sound too good to be true.



Visit <http://staysafeonline.org/ncsam/>

STOP

Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, your family's safety, or that of your colleagues.

CONNECT

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer or mobile device.

PHISHING ... DON'T GET HOOKED BY AN EMAIL SCAM !!!

Recently we have experienced a high volume of phishing emails. When you read email or surf the internet, you should always be wary of scams that try to steal your login credentials or personal information. Many of these scams are known as "phishing scams" because they "fish" for your information.

There are several types of phishing scams. Scams that ask you to ...

- Respond to an email with your account password in order to prevent immediate closure of your account, confirm your account, perform security/system update, increase mailbox size, etc.
- Click on a link to a fake site and log in with your password to verify your account.
- Open a malicious attachment.

Please keep in mind that CCPS will never request your login information or ask you to confirm your account by completing an online form and submitting it. If you receive an email asking for your password or login credentials, delete it immediately, and never reply with your account information.

Any member who has responded to a phishing email or provided their login credentials via an online web form is advised to **IMMEDIATELY** change your password <https://ua.collierschools.com:8444/CCPS/jsps/login/Login.jsf> and notify the helpdesk (ext. 70445) of the compromise.



PASSWORDS

- Create good cryptic passwords that can't be easily guessed.
- Don't share your passwords or private account information, and avoid writing them down. This includes co-workers and supervisors.
- CCPS will never ask you for your password. Neither should any reputable service provider.

PC SECURITY

- Secure laptop computers and portable devices at all times.
- Always shut your computer down properly before leaving.
- Log off of, lock, or put your computer to sleep before leaving it unattended.



YOU *are the* target

INTERNET

- Be cautious when using the internet.
- Also, just opening a malicious web page can infect your computer system. Be aware of where you are going before clicking on a web link.
- Don't provide sensitive information to internet sites, surveys, or forms unless you are using a trusted, secure web page.
- Be certain you don't put sensitive information in locations that are accessible from the Internet.

EMAIL

- Never assume that email and/or attachments are private or confidential.
- Don't open email attachments or click on links in emails unless you really know what you're opening.
- Delete suspicious emails. Do not open, forward, or reply to them. Immediately delete the email or move it to your "junk mail" folder to prevent more messages. Once you have deleted the email, make sure to empty your recycling bin.
- District email is for business use only.

OFFICE

- Secure your area, files, and equipment before leaving it unattended.
- Lock up sensitive materials.
- Dispose of data sensitive/confidential document properly.
- Be aware of visitors. Always escort visitors to their destination or to the security desk if you cannot assist them.
- Practice proper telephone and email security to ensure non-discussion of confidential or sensitive information in private areas. Never share or discuss confidential data with unauthorized individuals.

REMINDERS

- Think before You Click
- Use Hard to Guess Passwords
- Avoid Phishing Scams
- Shop Safely Online
- Protect Your Identity
- Dispose of Information Properly
- Protect Your Children Online
- Protect Your Portable Devices
- Secure Your Wireless Network
- Back-Up Important Files