***Popcykol* Presentation by Teressa Gehrke, Saturday, November 12, 2022 to AAUW Littleton-South Metro [*Notes by Mary Lynn Korch, branch member.* Summary reviewed by Teressa Gehrke January 2023]**

Website – https://www.popcykol.com

I have found, on this website, the most enlightening information under Security Appearances but it does tend to be somewhat technical.

At her presentation to AAUW LSM, Teressa shared a great deal of information. *I cannot profess to have taken complete notes, but I picked up a packet of information from Popcykol that is broken down into pages, included here as follows [MLK]:*

TIPS – All About Passwords

TIPS – Multi-Factor Authentication (MFA) Also known as 2 Factor Authentication (2FA)

TIPS – Netiquette which is using good manners and behaviors online

TIPS – Metaquette in the Metaverse. (The Metaverse is a shared virtual, 3D space in which a real person can interact with other people, known as *avatars*, objects and environments in virtual reality.

TIPS – Phishing which is a type of social engineering where an attacker sends a fraudulent message designed to trick someone into revealing sensitive information or to deploy malicious software (malware) on the victim's device.

Phishing TIPS are followed by a Sample Phishing Email and a marked-up Email asking you to Spot the Red Flags in the Phishing Email (2 additional pages.)

TIPS – Cyberbullying is like regular bullying but done on a computer and online.

Passwords – the speaker shared a chart that showed how to create a password that included, preferably, at least 12 characters comprised of Capital letters, small letters, numbers and a character such as #, @, &, etc. She showed that passwords of 12 or more characters are the hardest to "guess" and that ones of 18 characters are extremely secure.

She recommended that you 1) NEVER share your passwords with anyone; 2) Use a different password for each online account; 3) Change your passwords regularly

but immediately if you believe that your account has been hacked or phished; and 4) Use a Password Manager, which is a tool to safely and securely manage your passwords.

There was a lot of discussion about managing passwords, creating unique passwords for every online account and safety and security. *I did not take complete notes on the entire discussion regarding passwords. [MLK]*

Multi-Factor Authentication (MFA) – Probably most familiarly used in banking applications. It usually needs to be enabled and the verification comes as a SMS (Short Messaging Service) through a text on your phone, a number/code sent to your email. In some sites or applications, you can go to the Privacy or Security Section of the site and enable this feature. There are sites, most often financial or banking sites, that frequently require MFA or 2FA.

(Unverified by me) On your phone there are applications that you can 'turn on' to set the requirement for an authentication code. On the iPhone or Android, it would be found, respectively, in the Apple Store or Google Play, something like a Google Authenticator.

Phishing and Ransomware – as mentioned, Phishing is usually a fake message designed (often quite cleverly) to trick someone into revealing sensitive information. Once your account has been hacked (usually after you are tricked), the hackers frequently follow up by accessing your account and installing Ransomware. Definition from an IBM website: Ransomware is a type of malware, or malicious software, that locks up a victim's data or computing device and threatens to keep it locked — or worse — unless the victim pays the attacker a ransom. In 2021, ransomware attacks represented 21 percent of all cyberattacks (PDF, 4.1 MB) and cost victims an estimated USD 20 billion overall (link resides outside ibm.com).

An often reported (usually after the fact) ransomware attack is to hospitals and municipalities. A staff member inadvertently opens (clicks on) a link which exposes the information data system of the hospital, business, city, county, etc. to the hacker who then can install the ransomware and take over the said system, locking it and demanding money to unlock it.

Vishing - Other forms of this type of intrusion into a user's private, sensitive information can include "Vishing" which involves fraudulent calls or voice mails requesting personally identifying information (PII.) Professional advice regarding Vishing is to never share your personal identifying information over the phone to avoid a "man in the middle" attack and DO NOT call unknown numbers back.

Smishing – the use of text messages as a form of "Phishing." Often involves mass texts which direct the user to a malicious site to get information like personal identifying information. (MLK: Unfortunately, I wrote a note that says "turn off caller ID on Androids or iPhones." I do not know whether that can be done externally by someone who is "smishing" and I cannot imagine why a user would want to do this. I always want to know if the number is a known or unknown one. But I understood subsequently, that it turns off your caller ID.) *Per Teressa G. "I searched this and, on an Android, you can look up caller ID settings. Under Call Settings>Supplementary Services you can "Show your caller ID" and toggle between Network default, Never, and Always.*

Per Teressa G. Here is a current link to modify caller ID on iPhones: https://www.laptopmag.com/how-to/how-to-hide-caller-id-on-iphone-make-anonymous-phone-calls

Notes re: phishing and related vishing and smishing – You can avoid phishing by updating your security links. You can type in the whole website in your browser and/or look for: 1) time of day (usually late night early morning is a bad sign); 2) spelling errors; 3) urgency of request (e.g., less than 24 hours, etc.); 4) directive to click on the link provided.

One good example that was given was, for instance, that your child was completely immersed in a game of Minecraft late at night, and a "phishing" link popped up saying that they will be cut off from the program unless they click on a link to renew the license or play. Without thinking, the child clicks on the link because she/he wants to continue playing and immediately the outside hacker has access.

To safeguard your PII, you can purchase filters that will reduce spam email that have phishing links through moving to a "virtual private network." One such filter can be found at *nordvpn*.

On the www.popcykol.com website, there is additional information relating to these topics. Teressa G. mentioned that one way to check to see if you have been targeted is by typing in *"haveibeenpwned.com"* and following the directive to enter your email or phone number. [Have I Been Pwned? (HIBP: with "Pwned" pronounced like "poned," (or pronounced like "owned" but with a p) and stylized in all lowercase as "have I been pwned?" on the website) is a website that allows internet users to check whether their personal data has been compromised by data breaches. The service collects and analyzes hundreds of database dumps and pasts containing information about billions of leaked emails and phone numbers.]

Hide my email – discussion among members included an option, often offered on online retail sites, to "hidemyemail" when setting up your accounts.

Unsubscribe – use this ONLY IF you have subscribed. Don't take the bait if you have not previously subscribed.

Banking/Financial information – tips to address a possible breach of your banking, credit, debit cards include:

1- Contact your bank/card issuer immediately
2- Explain "what do I want to do"
3- Report the breach to all three credit bureaus
4- Deactivate your bank card(s)
5- Consider a temporary* credit freeze
6- Change your password(s)
7- Implement MFA/2FA (multifactor/2 factor identification)

*Keep track if you have frozen your credit because, while frozen, you will not be able to make purchases (home, car) of any type when your credit record cannot be accessed by a lender. You must actively unfreeze your accounts in these cases.

Unofficial notes by Mary Lynn Korch, member, AAUW Littleton South Metro

There are two additional pages following the information from PopCykol included herein; What tricks are scammers using? (Learn how to spot a scam) and Protect Yourself (Tips to keep you and your money safe.)

TIPS

All About Passwords

What is a password? A secret word or phrase that protects your information online.

Why do we need a password? We need a password because we are trying to protect our personal information. It's private.

When do you need to use a password? Use a password when you need to access information for school, banking, email or social media accounts, apps on a phone, and other private information.

Where do you use a password? You may need to use a password on any website that asks for it. The password should be different for each new account you create or site you access. Having the same password for multiple sites is bad. If someone tries to break into your account with a password that is used across multiple sites, then they can access **ALL** your accounts and your private information. They should be different for each site.

How do you make a strong password? Use a combination of big letters, small letters, numbers, and special characters. If you forget your password, you can reset it. Strong passwords are typically 10 or more characters long. You can also use a passphrase, which is a long string of phrases put together, like "MyFavoriteiceCreamisRockyRoad".

How should you store your password? Do you have your passwords saved in a Word document or Excel spreadsheet? That's not a safe way to secure your information, even if the file is locked with a password, also known as encrypted. The password can still be stolen by a bad hacker. PopCykol recommends using a Password Manager. A Password Manager securely stores accounts, usernames, and passwords. When you need to log into a site, the Password Manager can enter usernames and passwords automatically. There are several Password Managers to choose from.

Don't use personal information in your password, such as:

- Username, first name, last name, nickname, birth date, or pet's name.
- Don't use a word common in English or foreign language dictionaries.
- Don't use simple alphabet sequences, like abcdefgh; qwerty; or the word "password" for your password.
- Don't use a simple number sequence, like 1234567
- Don't share your password with people who shouldn't have your password.

TIPS

Multi-Factor Authentication (MFA)

What is a Multi-Factor Authentication? MFA stands for Multi-Factor Authentication. It is also called 2FA or Two-Factor Authentication. MFA is an additional way to secure things like emails and banking. You can use it to get into a bank account online, your social media account, business/retail websites, and your emails.

Why is MFA important? MFA adds an extra layer of protection from a bad hacker who wants to steal your information, like Personally Identifiable Information (PII). It includes things like your name, address, birthdate, email, address, and Social Security Number (SSN).

When do you use MFA? Use MFA when you need to access information for school, work, banking, emails, social media accounts, apps on a phone, and other private information.

Where should you use MFA? You should implement MFA on all sites you access, so long as the site has that feature, and most do.

How do implement MFA? The site you're visiting typically has a setting that will let you enable or turn on MFA, like Google, Yahoo, Amazon, and banking sites as well.

Once you enable MFA on a site, you will get a call, text message, or email to verify your identity and that you want to access that site. You can also use an authenticator, like Google Authenticator. The authenticator will provide a code of numbers and/or letters to input into the site to verify your identity and ensure you want to access the site. If you get a notification that someone is trying to access the site and it wasn't you, you can deny access. PopCykol recommends **immediately** changing your password to a strong password. See our **PopCykol Tips: All About Passwords**, for more information about creating strong passwords.

TIPS

Netiquette

What is Netiquette? Netiquette is having good manners and behaviour online. Netiquette means internet or network etiquette. Think about the Golden Rule and treat others like you would want to be treated, but online.

Why is Netiquette important? Netiquette is important because you want people to perceive your behaviour as kind and acceptable, especially online. What you say and do can positively or negatively impact others, but it can also help or hurt you depending on how you treat people.

When do you use Netiquette? The short answer is any time you're online and interacting with others. Netiquette is for all ages.

How should you act online?

1. Always be kind to one another
2. Remember once you write it and share it with others, you can't take it back.
3. Just because you delete it, doesn't mean it's gone forever.
4. If you're in an online/virtual meeting, look at the camera lens, rather than the screen. It looks like you're maintaining eye contact when you look at the camera.
5. Don't spin in your chair, it can be distracting to others in an online/virtual meeting.
6. Know when to mute and unmute your microphone.
7. Set up an online/virtual meeting profile picture with a clear, nice-looking photo of yourself. This might be the first impression people get of you, especially if you're off camera or have stopped your video.
8. When you enter a meeting, greet people.
9. Don't use all capital letters in messages. It looks like you're SHOUTING!!!!!

TIPS

Metaquette in the Metaverse

What is Metaquette? Metaquette is having good manners and behaviour online while in the metaverse. Consider the Golden Rule and treat others like you would want to be treated, but online.

What is the Metaverse? The metaverse is a shared virtual, 3D space in which a real person can interact with other people, known as *avatars*, objects, and environments in virtual reality.

Why is Metaquette important? Metaquette is important because you want people to perceive your behaviour as kind and acceptable, especially in the metaverse. What you say and do can positively or negatively affect others. This new environment has fewer rules, and you should start in a positive, respectful mental and emotional space when interacting with other avatars. PopCykol is "**Building Kindness in the MetaVerse**".

When do you use Metaquette? Use Metaquette any time you're online and interacting with others. Metaquette is for all ages within the metaverse, whether it is at a virtual concert, virtual shopping, building teams and collaborating, hanging with friends, or exploring the space.

How should you act while in the Metaverse?

1. Always be kind to one another
2. When you enter a virtual space or meeting, greet people.
3. Remember once you write it and share it with others, you can't take it back.
4. Your reputation may precede you if you're behaviour is unkind, rude, or disrespectful.
5. Know when to mute and unmute your microphone.

Familiarize yourself with the metaverse. Ask a parent/caregiver about what they would do if they were in a virtual space. Reach out to PopCykol for more information or help.

MetaQuette

TIPS
Phishing

What is Phishing? Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick someone into revealing sensitive information to the attacker or to deploy malicious software (malware) on the victim's device, like ransomware.

Who gets phished? Everyone has had an experience with phishing. At first, it's hard to recognize a phishing email, phishing link, or a suspicious attachment. However, once you know the signs of a phishing attack, you are less likely to click on something suspicious.

What happens to the person's data once they're phished? Phishing enables a criminal to access your banking and social accounts to steal your identity. It can compromise your data and even lock you out of your accounts. Ransomware can occur and you may have to pay money (or pay in cryptocurrency) for your data to be decrypted and unlocked.

How can phishing impact children's information? With more children online for school, gaming, and participating in virtual reality, they are prone to giving out more information than they should and also receive scam communications via phone, email, and text messages with malicious links and attachments.

Here's an example of phishing

A child may receive a phishing communication via email or a text on their phone. The message could appear to come from a gaming platform like Xbox or Roblox offering a cheat code or coupon. All a child would have to do is click and enter their username and password on the platform and then the sender would then steal information and use it for their own purpose. Hackers often use spoofing to fake the sender's email address.

SAMPLE PHISHING EMAIL

To: johndoe@gmail.com
Subject: Your Minecraft account is suspended
Date: February 14, 2022 **Time:** 12:34 am

Dear Customer:
We regret to inform you that your account has been suspended due to continued harassment online of other users. A complaint was filed on January 23, 2022 by another user.

In order for your account to be unlocked, please click on the link to contact Technical Support. You must do this within 24 hours from the time of this message.

Minecraft Support Technician Speciulist
677 Fifth Avenue
New York, NY 10022-4210
www.minecraft.com

NOW, SPOT THE RED FLAGS IN THE PHISHING EMAIL

To: johndoe@gmail.com
Subject: Your Minecraft account is suspended
Date: February 14, 2022 Time: 12:34 am ← **Note the odd time of the sent email**

Dear Customer:
We regret to inform you that your account has been suspended due to continued harassment online of other users. A complaint was filed on January 23, 2022 by another user.

In order for your account to be unlocked, please click on the link to contact Technical Support. You must do this within 24 hours from the time of this message. **Sense of urgency created. If you hover over the link, it's misspelled. And the "o" is really a 0, which is suspicious spelling and usage.**

Minecraft Support Technician Speciulist ← **Specialist is spelled incorrectly.**
677 Fifth Avenue
New York, NY 10022-4210
The address is not a valid address. It is a Microsoft office, but not related to Minecraft support.
www.minecraft.com ← **This link is not accurate and leads to an incorrect URL.**

How can you avoid being phished?

- Ensure your computer and network is updated and patched with the most current updates from the computer vendor.
- Avoid clicking on links when you're not sure of the sender.
- Even if the sender is a trusted person, are you expecting a message, text, or email from them?
- Type in the whole website in your browser instead of clicking it.
- You can purchase filters that will reduce spam mail that have phishing links.
- Phishing emails are getting more sophisticated and professional looking, however, are you expecting a message from the sender? Are they creating a sense of urgency?

How can I check if my email or phone number has been compromised?
Visit the site: **http://haveibeenpwned.com** to check.

TIPS
Cyberbullying

What is Cyberbullying? Cyberbullying is like regular bullying but done on a computer and online. Bullying is making fun of someone because you don't like what a person looks like, what they say or do.

Why is Cyberbullying bad? When you use unkind words, you hurt other people and when you use a computer to post mean words, messages, emails, and texts, they never go away, even if you delete them.

Where does Cyberbullying occur? Cyberbullying can occur at any time, like at school, work, on social media sites, like Facebook, Instagram, TikTok, Snapchat and more. It can happen on message boards/forums, like Reddit, Slack, and Discord.

How can we be kind online? Instead of getting mad at someone. Let's calm down. Take a long, slow breath. Do that before you write something. Because once we say something mean online, we can't take it back. Even if we delete the message or text, there's ALWAYS a record of it somewhere. Mean messages never go away.

What happens to the person who is cyberbullied? Their feelings get hurt. The person can be injured, or worse, they could die. When you use unkind words, what you really do is really put the meanness inside yourself.

Who can you trust to tell if you or someone you know is being cyberbullied? Try telling a parent, teacher, principal, or a coach. A grownup you trust should help you.

What if you're the one writing the mean stuff? Mean messages never go away even if you delete them. You can get in trouble with your parent, school, employer, or something more serious like with the police or FBI. Stop and take a moment to calm down before you say something you can't take back, and you get in trouble.

What tricks are scammers using?

Learn how to spot a scam

Scammers often pretend to be someone they're not. They may trick you into providing information to gain access to your account. Get to know the following scams to help keep your accounts safe and secure.

Online Shopping

A scammer sets up a fake online store and asks you to pay in ways other than a credit or debit card, leaving you without recourse when the item doesn't arrive.

Pay Yourself

A person pretending to be a Chase employee asks you to transfer money to yourself to resolve fraudulent activity.

Grandparent

Someone impersonates a loved one in crisis like claiming their car broke down or they lost their wallet and they need money right away.

Tech Support

A scammer requests access to your device to fix a technical issue, but really, they're collecting personal information.

Utility Shutoff

A person may pose as a utility employee saying your service will be stopped unless you pay them immediately.

Romance

A scammer creates a fake profile to gain your trust then asks for money for a health crisis or other bogus scheme.

Protect yourself

The following tips can help keep you and your money safe.

Guard your personal information

Don't offer information to someone who calls you directly, even if they say they're from Chase. When in doubt, call us.

Don't act immediately

Scammers may pressure you to pay them quickly and can have a demanding tone. Remember to take a moment, verify who they are and think about what they are asking for.

Use caution when sending money

Scammers could tell you to pay in ways where you may not be able to get your money back, like money transfers, gift cards or using Zelle®[1]. Always verify who the recipient is before sending money.

The way you pay matters

Different payment methods offer different protections. Chase debit and credit cards can help give you peace of mind with protections like fraud monitoring for unusual purchases.