Vista Royale Computer Club

February 17, 2022

Mike Johnson welcomed everyone; we have 64 members now. He drew for 2 giveaways from ACT Computers; here are the winners:

Aluminum ACT insulated cup water bottle, value $25 won by Tony Roach

Electronic Device Tracker, value $25 won by Carolyn Johnson

Our presenter Vicky Getz gave us her Part 2 of Spoofs & Spam and here are her detailed notes. She showed us some phishing examples and reviewed how to read URL's for domain names when following links as well as looking at the spammer's email address.

Cyber Criminals

Cyber criminals use your ignorance and/or inattention to:

- Trick you to enter information into look alike sites
- Direct you to malicious sites to do a drive-by infection.
- Trick you into downloading and opening malicious files.

What is a URL?

A URL (Uniform Resource Locator) or web address the address of a given unique resource on the Web. Https://www.google.com is a URL. URL's can be long and complicated, and many people don't know how to read them which can lead to them easily being taken advantage of. There are two parts of the URL that you need to pay attention to, the domain name and the connection method.

==========
DOMAIN NAME
==========

Domain names are unique and registered to a company or an individual for a period of 1 to 10 years.

The DOMAIN NAME IS THE IMPORTANT PART OF ANY WEB ADDRESS. The domain name is the only part of a URL that is registered and regulated.

URL's can be long and complicated. The DOMAIN is the part of the URL just to the left of the first single slash.

Https://subdomain.subdomain.domain.topleveldomain/folder/subfolder.document.e

Domain Name parts are separated by periods. The domain name is typically two parts, but can be three parts if it ends in a 2character country code.

DomainName.TopLevelDomain/

Https:// Ebay.com/

DomainName.CountryCode/

Https:// Ancestry.ca/

DomainName.TopLevelDomain.CountryCode/

Https:// Ebay.co.uk/

The top-level domains of .GOV and .EDU are the only domains that have restrictions as to their use.

The only restriction on other types of domains is that they are not already registered to someone else.

Subdomain

Subdomains are the portion of the URL preceding the domain name

Subdomains are usually used to offload tasks to another server.

Subdomains can also be used to mislead people.

Example

> https://support.hp.com/
> **HP.com** is the domain
> **Support** is the subdomain
>
> https://hp-laserjet-pro-400-printer-m401-series.printerdoc.net/
> **printerdoc.net** is the domain**hp-laserjet-pro-400-printer-m401-series** is the subdomain
> This site is not a genuine HP site!

QUESTION: Are URL's case sensitive?

The portion of the URL to the left of the first single slash (/) is not case sensitive.

The portion of the URL to the right of the first single slash (/) **is** case sensitive unless the website is using a Microsoft server.

==========
SECURE VS SAFE

Connection type
==========

HTTP:// stands for **H**yper **T**ext **T**ransfer **P**rotocol

An HTTP connection is not suitable for entering private information such as credit cards, login credentials, Medicare numbers, social security numbers....

In 2021, many browsers changed the symbol for HTTP from an open lock, to an exclamation point! and the words NOT SECURE causing many of our members to think that our website vrcc.info was not safe.

Not secure, does not mean unsafe.

It just means that the communications are not encrypted and a third party has not verified that you are on is the site reflected in the URL and NO CREDIT CARD or PASSWORD information should be sent through an HTTP connection.
VRCC.INFO never asks you for login information, nor credit cards...

HTTPS:// stand for **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure

A lock is displayed on the URL indicating it is an https connection.

Secure does not mean SAFE

Secure means an SSL certificate has been issued verifying ownership of the domain and ensures the domain displayed in the URL is in fact the domain you have reached and communications are encrypted so the information cannot be intercepted by some other entity on its way over the internet.

More and more criminal organizations are opting to get an SSL for their domains.
A HTTPS connection combined with the wrong domain can be very unsafe!

========
PHISHING
========

When scammers send you emails and text that direct your malicious sites or send you attachments designed to steal your personal information, this is called phishing.

They may:

- Claim there is suspicious activity on your account
- Claim there is a problem with your payment
- Send a fake invoice
- Claim you need to update your information
- Offer a limited time discount
- Offer a refund
- Ask you to take a survey

Phishing Scams usually involve something that:

- Scares you into quick action
- Angers you into quick action
- Lures you into quick action (a special deal)
- Lulls you into action because it seems so routine
- Asks for your opinion
- Sometimes they just impersonate your friends.

==========
EMAIL DOMAIN NAME
==========

Email addresses also have domain names.

On business correspondence the email domain should be the same as the business's domain. Scam emails usually come from personal email accounts, like @gmail.com, @aol.com, @outlook.com, @hotmail.com....

Major businesses use their company's domain in their email communications

@netflix.com, @wellsfargo.com, @att.com

Example: Netflix emails should come from a sender@Netflix.com

A simple check of the sender's email domain can help you easily identify a scam.

Note an email from AT&T is going to come from someone at ATT.COM. While an email from an AT&T customer will come from ATT.NET

=====
LINKS
=====

Email links can be hyperlinks, which means that the links can easily disguise the destination.

Links in texts are WYSIWYG, but if they are long URLs, they are often sent to a shortening service to fit into the SMS (Short Message Service) length restriction so many people are used to clicking on strange looking links in texts.

Look where you are going!

Links in phishing emails take you to malicious sites to trick you into entering information or deliver drive-by malware.

The descriptive text or pictures in a hyperlink may be misleading.

But it is easy to look at the destination web address before you follow a link and see if the domain looks suspicious.

On a PC Hover

When your mouse pointer moves over a link, your cursor changes to a hand. The destination web address will appear in the lower left-hand corner of your browser window.

On Tablet or Smartphone

A long press on the link reveals the destination just like hovering did on a PC. The long press on a link works with links in browsers, emails, and text messaging.

Good Habits

> Never follow links or use phone numbers contained in emails or texts that require you to take action on your accounts.
>
> Always use web addresses and main phone numbers you KNOW are real.
>
> If possible, use saved Bookmarks or Favorites to navigate to your account websites to avoid typo-squatters.
>
> ==========
> MASS MAILINGS
> ==========

If you signed up for a mailing list that you no longer wish to be a part of, you may unsubscribe.

If you didn't sign up for that mailing list, MARK IT AS SPAM, DO NOT UNSUBSCRIBE as that will take you to that site that you think is malicious anyway. At the very least the spammer now knows your email address, what kind

of computer/phone/tablet you use for your email, what OS version it runs, what browser and your IP address, who your provider is, and your general location.

==========
ATTACHMENTS
==========

Attachments can be very dangerous. Attachments from strangers should never be opened.

Spammers will try to trick you into opening an attachment by displaying your friend’s name.

But attachments from friends who have been hacked can be just as dangerous.

Make a practice of looking at the sender's raw email address before opening any attachment.

Do NOT open attachments you are not expecting.

Some Simple Rules

- Look at the sender's real email address if the message contains links or attachments.
- Look for the domain and connection method before you click a link.
- Do not use links or phone numbers for emails that require action on your account, always use known phone numbers and web addresses, use bookmarks/favorites if possible.
- Do not open unexpected attachments.

==========
PRACTICE PASSWORD FIDELITY

==========
NEVER REUSE YOUR PASSWORDS OVER MULTIPLE ACCOUNTS!

QUESTION: Do you recommend a password generator?

Password generators create complicated passwords, that are extremely difficult to remember and type, but are no safer than a long random phrase from a brute force attack. I use long phrases, that include numbers and symbols. Since I started using mobile devices, I now use the numbers or symbols at the beginning or end of the passwords to make them easier to type on the glass surface of a tablet/smartphone where you have to switch keyboards to get to your numbers and symbols. The issue with my method is that a shoulder-surfer can read and

memorize your password easily, just ask my granddaughter what my ATT password is, lol.

Stay tuned for next week.....

Regards, Sandy McKenny, Sec