National RTAP
Rural Transit Assistance Program

Cybersecurity 101 Webinar – Summary and Q&A

February 11, 2021

KEY POINTS

- A primary cybercrime strategy is getting you to click on links or attachments in emails and on websites, which then can put viruses on your computer and get the hacker inside your computer or network. This can be very costly. To avoid this, you should do the following:
    - Be very careful clicking on links in emails and downloading attachments, especially zip files. If anything says "Click Here," you probably need to delete it.
    - Emails that try to scare you, are overly intriguing, too good to be true, or promise you something are suspicious and should be deleted. Never click on anything in these emails.
    - Be aware of fake emails with invoices or tracking numbers. Scammers are very smart and these emails often look legitimate! Fake emails from Amazon saying "click here to track your shipment" have been known to be clickbait for criminal activity.
    - When in doubt, double check the email sender, call them to verify, or just delete the message.
    - Do not click on online ads and other sponsored content. Criminals know everyone wants to see celebrity gossip and if you click on those links, it could be a virus.
- Another cybercrime strategy is guessing or stealing passwords.
    - Make your passwords strong. Especially for your computer, email, online banking, and home Wi-Fi. Using phrases, song lyrics, etc. is a good idea, with symbols or numbers mixed in. Something you can remember ideally.
    - To keep track of your passwords, a strong password-protected Excel file is an option.
- Other important tips:
    - Avoid public Wi-Fi! Especially when entering your credit card number or other sensitive information. Someone can easily see what you are doing and steal your information.
    - Be careful when shopping online. Avoid paying with your credit card online if possible. It is better to use PayPal or other similar services. And never use your debit card to shop online.
    - Use a separate computer for important tasks like online banking only, if possible, and another computer (or better yet, a tablet/smart phone) for other activities like social media, especially if you have kids.
    - Never email sensitive information, like your social security number, credit card, or passwords.
    - Use two-factor authentication if you can (see more below).

WEBINAR Q&A

Can you recommend a security system for a home computer?

- Anti-virus software isn't as effective as it used to be, although it is better than nothing. Artificial intelligence is best, although hard to buy for a personal consumer. You may want to call your

company's IT department and ask if they can install the same software used for the company's networks/computers for your home computer, and offer to pay them for the cost.
- But if you must buy something retail, Webroot is pretty good[1].

Is two-factor authentication effective?
- Two-factor authentication is very effective in increasing your security, because anyone trying to login to your computer or account would need your phone to do so, not just your login and password.
- An example of two-factor authentication is when you are required to enter a code that was either emailed or texted in order to log into an account. This is commonly used for logging onto your bank's website. It can also be set up for logging onto your computer, email and more.

How secure are payment options like PayPal, Apple Pay, Samsung Pay, etc.?
- They are a better option than entering your credit card on multiple sites.
- If a website doesn't take PayPal or something similar, it may not be a company with good enough security or legitimacy to warrant the risk of buying from them online.
- Never enter your debit card online. If they get your debit card, they can get direct access to your money. With a credit card you are more protected.

What password manager do you recommend? Or what is your recommended strategy for keeping track of passwords?
- Password managers are helpful, but they can be hacked. For example, LastPass, a popular password manager, was hacked. Almost anything can be hacked.
- One strategy is to have a password protected Excel sheet. Again, use a robust password.
- Using phrases that you can remember is best, with some numbers and/or symbols mixed in. You want it to be strong, but something you can remember so you don't have to reset it constantly.

How often do you change your passwords?
- It depends on the account, but generally three times per year.
- It is most important to keep passwords strong and memorable.

Are there any risks with using a Virtual Private Network (VPN)?
- There are the same risks with a VPN, in the sense that if a hacker gets into your computer, they have access to the VPN network. It is important to have strong passwords for your computer and VPN.

Can home security cameras or cameras on computers/phones be hacked?
- Anything connected to the internet can be hacked. If a hacker can get into the computer, or another device connected to the camera, they can control the camera.
- The best thing to do is to have strong passwords for your computer and any accounts related to internet-connected devices.
- To be safe, you can always cover cameras or web-cams with a post-it.

How secure are internet-connected devices at home (e.g., smart fridge or thermostat)?
- They are not very safe. Software in those devices is not updated often, the way it is on a computer or cell phone. If you have "smart" devices in your home, be sure to have a very strong Wi-Fi password and secure Wi-Fi.

[1] National RTAP does not endorse any specific outside products or services.

How safe are smart phones?

- Currently, phones are considered safer than computers in terms of hacking. However, it is recommended to set your phone to auto-lock after a minute and to be careful what you click on. And avoid public Wi-Fi, especially for doing online banking or making a purchase that requires a credit card.

Is it safer to use an app on your phone or go to a company's website in a browser?

- It doesn't matter as both are equally are safe. What matters is not to use public Wi-Fi. It is always safer to use data (cellular/LTE/4G etc., anything not on Wi-Fi). If possible, try to have an unlimited data plan so Wi-Fi is not needed.

What is social engineering?

- In the context of cybersecurity, it is the use of deception to manipulate someone into sharing confidential or personal information for fraudulent purposes.
- An example is "whaling" or CEO fraud, where a cybercriminal masquerades as a senior player at an organization and directly targets important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes. For example, criminal pretends to be a new client, learns about the company, emails the CEO to learn their writing style, sets up a similar website/email, and writes emails as if they were the CEO asking staff for sensitive information or with links to malware disguised as something else.