System IT Board Report

November 8, 2023

Cyber Security Awareness

October was Cyber Security Month, so it seemed fitting to share with the Board some of the information that was shared with all CCCS employees via a series of cyber security awareness emails during October outlining good cyber security practices and general cyber security information. Many thanks to our Manager of Information Security, Gaven Memmen, for putting all this information together for CCCS employees. All CCCS employees also take an online cyber security training each year.

Passwords

Passwords are now an important part of everyday life. Today we need them for everything from accessing our smart devices to our banking information, not to mention all the passwords we use at work. To better protect our accounts from being compromised, it is important to use strong and secure passwords.

A few things to keep in mind regarding passwords security:

Do's:

- Make sure your password is at least 16 characters
- Use a mix of upper and lowercase letters, symbols, and numbers

Don'ts:

- Include personal data, such as birth year or pet name
- Sequential numbers, such as 1234
- Repeated numbers, such as 8888
- Keyboard patterns, such as QWERTY

Other Tips:

- **Passphrases**: Consider using a passphrase for your password. Passphrases make it easy to create rememberable complex passwords. Click here to learn more about passphrases.
- **Never reuse passwords**: There is the possibility that your password may have already been compromised due to a data breach, and cyber criminals have obtained it. Therefore, it is important to never reuse passwords. You can use this popular website to check if your credentials may have been leaked: https://haveibeenpwned.com/
- **Enable Multifactor Authentication (MFA)**: Enabling MFA provides an extra layer of security, making it more difficult for cyber criminals to access your accounts. However, be cautious of any MFA prompt you did not request, this may indicate that a bad actor has gotten a hold of your password and is trying to access your account. If you receive

unexpected MFA prompts, you should change your password. Click here to find out more about enabling MFA.

- **Use a password manager**: Password managers can create complex random passwords, which will make it more difficult for hackers to compromise your accounts. A few password managers you may be interested in are:
  - https://www.keepersecurity.com/personal.html
  - https://bitwarden.com/products/personal/
  - KeePassXC Password Manager – (KeepassXC is free and installs locally on your machine but may have a slight learning curve for some users.)

For more information about password security, visit the following websites:

- https://www.cisa.gov/secure-our-world/use-strong-passwords
- Top Five Password Security Tips – Keeper Security

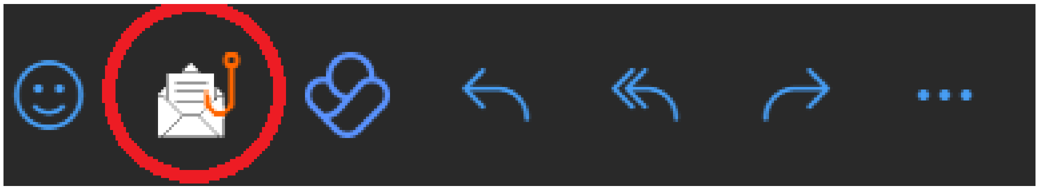
Key Takeaways:
Make sure your password is at minimum 11 characters with a mix of letters, numbers, and symbols. The graphic below demonstrates how long it would take to crack passwords of varying complexity. Remember the longer a password is, the more difficult it is for automated computer systems to crack. Click here to test your password knowledge.

Phishing

Let's take a look at how to thwart the many different ways bad actors try to phish us; whether it's via email, phone call, text message, or social media, be vigilant when clicking links or the information you share. Here are a few things to keep in mind when you are unsure about an email, text message, or phone call:

- **Always verify the person on the other end**: When receiving an unexpected request for information or a call to action, remember nothing is that urgent. You can take the time to verify the requestor by calling the **official** support number, or someone you are familiar with at the organization. Do not call the numbers provided in the message, and NEVER give unauthorized persons access to your computer.
- **Trust your instincts**: If something doesn't feel right, reach out and check with another team member or IT professional to verify your suspicions.
- **Think before you click**: Before clicking any links or files, make sure you verify they are legitimate; you can do this by hovering over links or email addresses to verify the URL. If you are ever unsure about the contents of an email, reach out to your IT team to help you verify.
- **Use the phishing or spam buttons**: Many email services provide a phish or spam button. These buttons help protect you and others who may have received the same email. I highly recommend reporting these to help email professionals identify pesky emails to keep our inboxes clean.

For simple and quick email reporting in our employee mail system, we use the Phish Alert Button located in our Outlook messages which sends the suspect email directly to our Security and Outlook teams.



The following links provide information on how to spot social engineering and phishing emails, and more detail on what to do to report them:

- Phishing - When You Report, We Get Stronger -- PAB
- Recognize and Report Phishing | CISA
- Understanding URLs
- How To Spot Phishing Emails - Keeper (keepersecurity.com)
- Pretexting - "Tech Support" Social Engineering

General Cyber Security Awareness
Security Culture:

- Take cyber security training seriously! Learning how to spot potential cyber-attacks helps to improve our overall security culture.
- Cultivate our security culture by helping others spot and respond to potential cyber threats.
- If you see something, say something; be sure to reach out to team members or IT staff if something doesn't seem quite right.

Passwords and MFA:

- Create strong passwords using password best practices.
- If possible, use a password manager to keep and create unique passwords.
- Use passphrases to create long and rememberable complex passwords.
- Enable multi-factor authentication (MFA) wherever you can.
- Never reuse passwords, and make sure all your passwords are unique. This includes incrementing numbers when creating or changing your password; for example, changing “password1” to “password2” is easily guessable by hackers.

Phishing and Social Engineering:

- Trust your instincts: If it feels suspicious, double check with a team member or IT staff.
- Verify email senders or suspicious callers: Don't be afraid to verify with a trusted source the email or phone call that you received was expected.
- Use the Phish Alert Button (PAB): This ensures the email team can clean up unwanted emails before they reach others, reducing the possibility of attackers compromising us.

Software Updates:
This wasn't covered in our weekly topics, but a very important part of security is making sure your software is updated often. Updates ensure any bugs and/or vulnerabilities found within software are fixed, reducing an attacker's ability to gain access or exploit systems. Make sure to:

- Turn on automatic updates wherever possible.
- Install updates as soon as you receive update notifications.

Click here to learn more about updating your software

Spread the word! We want to help you, your family, friends, and our community stay safe all year long. For more information about ways to stay safe online, check out these recommended resources:

- https://www.cisa.gov/cybersecurity-awareness-month
- Keeper Security Blog - Cybersecurity 101

Thanks for Celebrating Cybersecurity Awareness Month!