CYBERSECURITY TERMS

WHAT THEY MEAN AND WHY YOU SHOULD KNOW THEM

Cybersecurity threats and attacks are on the rise! Sadly, many people are unaware of the terms and tactics used by cybercriminals, leaving them vulnerable to cyber attacks. Here are common terms and tactics used by cybercriminals.

Social Engineering

This is a term used when trying to deceive or manipulate people to disclose confidential or personal information to be used for scams or fraud.

Solution: Stop and think about where the source of the communication is coming from. Does it make sense? You can always ask for ID and verify the sender, use a spam filter, like IRONSCALES that can help identify and block phishing messages, or think to yourself if this scenario is realistic. Most importantly, keep your guard up when engaging with anyone via email or SMS.

Phishing

Technique where an attacker creates fraudulent emails to misrepresent companies/churches in order to manipulate individuals to disclose personal or confidential information. i.e. credit card numbers or passwords.

Solution: Be on guard when receiving emails from unknown senders. Often, the email addresses will look slightly different from who they are pretending to be. Remember, NEVER click a suspicious on unexpected link.

Smishing

This is a term used for phishing attempts via SMS text messaging. Frequently, these texts come through posing as brands offering deals on their products. As a whole, people are less on guard when it comes to text messages because it is a more personal form of communication.

Solution: Treat suspicious/odd texts the same way you treat suspicious emails, do NOT click on links from unknown senders.

Vishing

This is a term used for voice phishing attempts via phone calls. The caller pretends to be a trusted source and tricks victims into revealing personal information such as bank details, passwords, or credit card numbers.

Solution: Be aware of unexpected calls asking for ANY type of personal information. If you think it might be legitimate, call the person or company back using a phone number you have on file (NOT a number they provide you).

Password Spraying

Technique where an attacker chooses a common, easy-to-guess password and goes through a long list of usernames until they get a hit and can access an account using said password. This is the most common source of automated account hacks.

Solution: Do not use common, easy-to-guess passwords! Use a password manager to help you craft strong, unique passwords for all of your online accounts.

ENABLE MINISTRY PARTNERS

CYBERSECURITY TERMS

WHAT THEY MEAN AND WHY YOU SHOULD KNOW THEM

Password Replay

Technique where an attacker takes credentials leaked at one company and tries the same credentials on other accounts, hoping the user reused the same usernames and passwords. 60% of users reuse passwords, but this is exactly why you should not recycle passwords.

Solution: Do not use the same password for multiple accounts, especially important accounts such as your bank or email.

Baiting

Technique where an attacker uses a USB stick which has been previously downloaded with malware and they convince you to insert this USB stick into your computer, giving access to hackers.

Solution: Don't use a USB stick that you find in the parking lot or randomly on your desk.

Pretexting

Technique where an attacker sneakily gains your attention and reels in personal information. This could be as simple as an online survey, information put out on social media, or an individual going around asking questions.

Solution: Be on guard and remember not to release personal information to strangers appearing to be important. Be mindful of the information you put out on social media.

Data Breach

The exposure of sensitive, confidential, or personal information by an unauthorized individual is a violation of security, otherwise known as a Data Breach.

Solution: Report the breach/attack. We encourage you to not delete or ignore the threat. All compromises should be reported to your IT support personnel so they can be documented, tracked, and responded to correctly.

Did you know 70-90% of all malicious breaches are caused by social engineering and phishing? Some of the most popular threats appear via websites and emails, all tricking church employees into disclosing confidential information. It is imperative to teach all employees how to recognize the most frequent signs of social engineering and phishing.

Be a team player by ensuring you are keeping your data secure! Remember to always think twice before clicking links from suspicious emails or texts and giving out too much information to an unknown caller.