#SeeYourselfInCyber

Strong Passwords

It may be easy to identify people who could gain physical access to your devices—family members, roommates, coworkers, people nearby, and others. Identifying the people who have the capability to gain remote access to your devices is not as simple—if your device is connected to the internet, you are at risk for someone accessing your information. However, you can significantly reduce your risk. .

CREATING A PASSWORD

Creating a strong password is a critical step to protecting yourself online. Use long, complex passwords for the best protection. No one is immune to cyber risk, but #BeCyberSmart and you can minimize your chances of an incident.

SIMPLE TIPS

Use a long passphrase. Best practice: consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.

Don't make passwords easy to guess, such as your names or your pets' names... This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

Avoid using common words. Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L."

Get creative. Use phonetic replacements, such as "PH" instead of "F." Or make deliberate, but obvious misspellings, such as "enjin" instead of "engine."

Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening more ways with which it could be misused or stolen.

Unique account, unique password. Having different passwords for various accounts helps protect you.. It's important to mix things up—find easy-to remember ways to customize your standard password for different sites.

Double your login protection. Use multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. Enable MFA by using a trusted mobile device,

such as your smartphone or an authenticator app.

Our world is increasingly digital and increasingly interconnected. So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on. Being cyber smart is contagious. Take the three of the basic steps outlined above and help two friends do the same.

Remember: always trust your instincts. If an email, phone call or an attachment seem suspicious, don't let your curiosity put your computer at risk! If you see or hear something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

Best regards to all,

Curtis Clan | Chief Information Security Officer, CISSP

You May Also Be Interested In:

CyberSafeTN

NCSAM Tips and Advice

Security & Risk Mitigation Resources

STS Security Services Policy Documentation