TN Department of Finance & Administration | Strategic Technology Solutions

2022 NCSAM National Cybersecurity Awareness Month

#SeeYourselfInCyber

Updating Software

This week's action step for cybersecurity awareness month also needs to be a focus year-round. While it may seem inconvenient to keep your software updated, ransomware or the theft of personal information is beyond inconvenient and we want to avoid that! It's much easier to keep your information secure by keeping your software updated.

WHAT TO UPDATE

Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too.

UPDATE OFTEN

When updates become available, don't delay. Always keep your software updated! These updates fix general software problems and provide new security patches to keep criminals out. You can be sure the bad guys are always looking for new ways to get to your data, so updating your software is an easy way to stay a step ahead.

GET IT FROM THE SOURCE

Get your updates ONLY from the company that created it. Never use a hacked, pirated or unlicensed versions of software (even if your friend gave it to you). These often contain malware and cause more problems than they solve.

MAKE IT AUTOMATIC

Software from legitimate companies usually provide an option to update your software automatically. When there's an update available, you'll get a reminder so you can easily start the process. If you can't automatically update it, remind yourself to check quarterly if an update is available.

WATCH FOR FAKES!

Pop-up windows on the web that tell you to URGENTLY do something are always fake and should not be followed. A browser will only warn you not to move forward or stay on a specific web address if it's not secured or it contains malware.

We want everyone to take ownership of the critical role we each play in protecting cyberspace, and the importance of taking proactive steps to enhance cybersecurity. Everyone has a duty to do their part,

whether on the job, at home, or at school—now and in the future. Cybersecurity must be a priority and not an afterthought. Actions taken today can affect the future of personal, consumer, and business cybersecurity.

Remember: always trust your instincts. If an email, phone call or an attachment seems suspicious, don't let your curiosity put your computer at risk, and try to avoid hurriedly going through your email because that's when you might click before thinking!! 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