October is National Cybersecurity Awareness Month and the Salt Lake Chamber is partnering with the STOP. THINK. CONNECT.™ Campaign, a national public awareness effort to guide the nation to a higher level of Internet safety by challenging Utahns to be more vigilant about practicing safer online habits.

As technology evolves, the prevalence of ransomware attacks is growing among businesses and consumers alike. It’s important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that accesses a victim’s files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code. Ransomware is like the “digital kidnapping” of valuable data – from personal photos and memories to client information, financial records and intellectual property. Any individual or organization could be a potential ransomware target.

WHAT ARE BOTS AND BOTNETS?

There’s no question that the internet is awesome; it makes our lives easier and connects us to the rest of the world. Unfortunately, there are bad guys out there who harness that convenience to do harm. One of the common types of cybercrime infects connected devices with specific types of malware, turning them into what are known as bots. Once a device becomes a bot, it is usually part of a botnet or a larger network of other infected devices that are all controlled remotely by hackers. Cybercriminals use bots for financial gain or to steal, send spam to infect more devices or attack websites. A botnet can have anywhere from a few hundred to many thousand devices at its disposal.

WHAT CAN YOU DO?

We can help protect ourselves – and our organizations – against ransomware and other malicious attacks by following these tips:

○ Keep all machines clean: Keep the software on all Internet-connected devices up to date. All critical software, including computer and mobile operating systems, security software and other frequently used programs and apps, should be running the most current versions.

○ Get two steps ahead: Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.

○ Back it up: Protect your valuable work, music, photos and other digital information by regularly making an electronic copy and storing it safely.

○ Make better passwords: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.