Cyber Threat, the Federal Bureau of Investigation (FBI) and Being Cautious When Connected on the Internet

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries. The FBI is the lead federal agency for investigating cyber attacks and intrusions. Whether through developing innovative investigative techniques, using cutting-edge analytic tools or forging new partnerships in our communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat.

TRTA members should be alert, aware and take the right security measures when connected to the internet. Everyday tasks – opening an e-mail attachment, following a link in a text message, making an online purchase – can open you up to online criminals who want to harm your systems or steal from you.

Protect Your Systems and Data. Keep systems and software up to date and install a strong, reputable anti-virus system. Create a strong and unique passphrase for each online account you hold and change them regularly. Do not open any attachments unless you are expecting the file, the document or invoice and have verified the sender's e-mail address.

Protect Your Connections. Be careful when connecting to a public wi-fi network and do not conduct any sensitive transactions, including purchases when on a public network. Avoid using free charging stations in airports, hotels or shopping centers. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices that access these ports. Carry your own charger and USB cord and use an electrical outlet instead.

Protect Your Money and Information.

Examine the e-mail address in all correspondence and scrutinize website URLs. Scammers often mimic a legitimate site and e-mail address by using a slight variation in spelling. Or an e-mail may look like it came from a legitimate company, but the actual e-mail address is suspicious.

Do not click the link in an unsolicited text message or e-mail that asks you to update, check or verify your account information. If you are concerned about the status of your account, go to the company's website or log into your account or call the phone number listed on the official website to see if something does in fact need your attention.

Carefully scrutinize all electronic requests for payment or transfer of funds.

Be extra suspicious of any message that urges immediate action.

Make online purchases with a credit card for an extra layer of protection against fraud.

Do not send money to any person you meet online or allow a person you don't know well to access your bank account or transfer money in and out.

Report Internet Crime to the FBI at ic3.gov .

If you are a victim of an online or internet-enabled crime, file a report with the Internet Crime Complaint Center (IC3) as soon as possible. You can also visit IC3 for more information including tips and information about current crime trends. You can also learn about common scams and crimes, as well as discover more about the work of the FBI's Cyber Crime Division.