CyberAlert

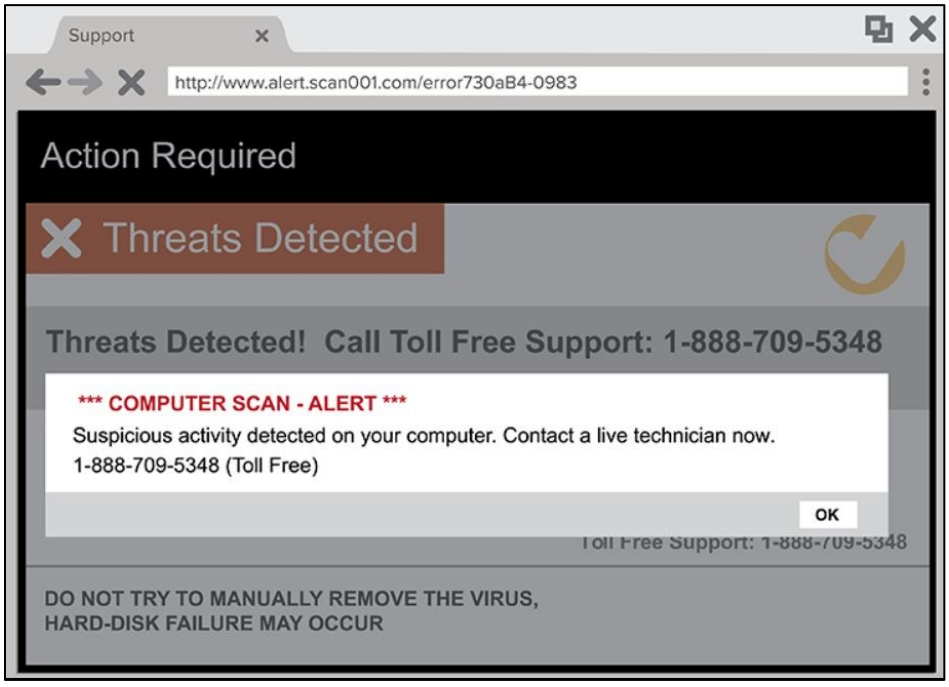
November 22, 2019

'Tis the Season for Tech Support Scams

Risk Management Question: How do you recognize and protect against tech support scams?

The Issue: Many will celebrate this holiday season by treating themselves or a loved one to the gift of technology. A shiny new smart watch, mobile device, or tablet may bring visions of convenience and enhanced productivity, but they can also bring risks if the device is not properly set up and protected. Scammers know the popularity of holiday technology gifts and will try to take advantage of anyone who is not vigilant. An owner of new or unfamiliar technology can be easy prey.

One common scam takes the form of a communication made to appear as if it's from a company's tech support team. The communication can take a variety of forms: pop-ups, ads (while using the new device to surf the web), phishing emails, and phone calls. The goal of the tech support scammer is to convince you that your computer or device has a serious issue, that you need to act quickly, and they are there to help you.



HINSHAW

Tech support scammers may claim or try to convince you:

- They need to connect to your device in order to run a scan or resolve an issue, but instead of fixing the problem, will install malicious software.
- To click on a link, or visit a website to be able to diagnose a problem with the device.
- To purchase a service or download an app to resolve a problem. Be especially wary of suggestions that you may buy the app, or pay for the service by wiring money or using a money transfer app. Scammers choose these methods of payment because they are difficult to reverse. And, if a tech support ever suggests you should use a pre-paid cash card, hang up. It's OK to be rude because you are likely dealing with a fraudster.

Risk Management Solutions:

1. Recognize that tech support scams are intended to catch you off guard. They try to create a sense of urgency in order to get you to act quickly and take advantage of your natural desire to keep your device and your data secure.
2. Never provide any information about yourself or your device in response to an email or call that you receive out of the blue.
3. Immediately change any default passwords or settings that accompany a new device.
4. Do not assume a malware pop-up is legitimate.
5. If you are ever concerned about a potential security issue with any of your devices, especially a new one, look up the vendor or manufacturer's tech support team and call that number, not the one in the warning.
6. Finally, if you get a pop-up message, use ALT-F4 on your keyboard, if possible, to close the window. Try to avoid clicking on the "X" or "CLOSE" button in a pop-up message because the malicious actor may have hidden malware in that button.

Enjoy your new tech device. And remember, always think before you click.

Happy Holidays from Hinshaw!

Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com

Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com