Keeping your organisation safe from mobile threats during the holidays

Digital transformation has pushed employees to use their personal devices for work. BYOD was previously a privilege extended to employees, but now becoming a critical component of today's business infrastructure strategy.

This problem is about to get worse as we enter the holiday shopping season as this season is a big event for cybercriminals.

Protecting your organisation from threats unknowingly brought in by employees requires a two-pronged approach. The first is to carefully harden your network from the fresh deluge of mobile device-related threats, and the second is to educate your employees on safe holiday shopping strategies.

Preparing your network

There are three basic security components that every organisation with an open BYOD strategy needs to be familiar with says Doros Hadjizenonos, regional sales director at Fortinet in South Africa.

1. **Secure mobile devices**: Where possible, you should establish a process for securing endpoint devices. First, if a user wants to attach their device to your network, there needs to be some minimum level of security they should have to meet. That should include installing some security app or client that can contribute to your overall security framework. Then baseline normal mobile device traffic so you can actively monitor and trigger alerts for any traffic anomalies.

2. **Secure the network**: Access points need to perform real-time threat analysis, including sandboxing, to detect malicious activity or software. That should be supported with a Network Access Control solution that can 1) identify and inventory devices, 2) assign them to an internal network segment based on device profiles and policy, and 3) respond to threats by quarantining infected devices.

3. **Tie everything together**: Endpoint security needs to be actively tied to your larger security architecture, including your NGFW devices, to ensure consistent policy orchestration and enforcement.

Help your users

Any effective security strategy needs to include a mechanism for training and counselling employees on safe device and internet usage. Here are a few messages especially relevant for the holidays:

Use caution when connecting to public Wi-Fi: Public Wi-Fi sites are a haven for criminals looking to intercept a connection and use it to steal passwords, banking or credit card information, and other personal data. Remind users that using a "Free Wi-Fi" access point may be connecting them to the Internet through a malicious device that can see and capture all the traffic moving between them and their online shopping site, bank, or social media accounts.

Only download legitimate apps from legitimate sites: Most mobile device infections are the result of downloading infected applications. Many of these apps hide on a device and monitor web and application traffic. During the holidays, when more online shopping occurs than any other time of the year, the chance that a compromised app can intercept financial or other personal information is especially high. Remind your employees to only download apps from legitimate application sites and never allow installations from "unknown sources."

Think twice before shopping at an unfamiliar site: Remind your employees that unusually low prices and high availability of hard to find items are red flags for scams. However, if they are going to shop at an unfamiliar online store, they should follow these four basic strategies to protect themselves, and by extension, your organisation:

• **Look before you click**: Before you click on a link, hover your mouse over it. This should reveal the URL address it is connecting you to. Look at it carefully. Is the name too long or does it contain lots of hyphens or numbers? Does it replace letters with numbers, such as amaz0n.com? If so, don't click on it.

• **Verify**: Start by entering the name of the site into a search engine to see if anyone has complained about it. Next, never click on a link from an unknown source. Instead, go directly to the site by typing in their primary address into your browser. From there, any legitimate retailer will provide you with access to any authentic deals advertised online.

• **Pay attention**: Once you connect to an online shopping site, take a minute to look at it. Does it look professional? Are the links accurate and fast? Are there lots of popups? These are all bad signs. Likewise, bad grammar, unclear descriptions, and misspelled words are other giveaways that the site is probably not legitimate.

• **Keep your distance**: Never use your debit card. If you decide to make a purchase, use a major credit card as most have built-in fraud protection. And as a bonus, they are not directly connected to your checking or savings account.