BIZCOMMUNITY

Employees must be educated about mobile cyber threats

By Doros Hadjizenonos

13 Feb 2020

While nearly 9 in 10 companies not only allow but actually rely on their employees to access critical business apps using their personal devices, according to a recent Fortinet Threat Landscape Report, Android-based malware now represents 14% of all cyber threats.

Doros Hadjizenonos, regional sales director at Fortinet

In addition to direct attacks, the number of compromised web sites, email phishing campaigns, and malicious access points continue to grow exponentially, infecting unsuspecting users – regardless of their devices – with spyware, malware, compromised applications, and even ransomware.

And whenever a personal device of any of your employees becomes compromised, they can represent an increased risk to your organisation as well. In addition to deploying mobile device management software and security clients to your employees, it is critical that you establish a cybersecurity awareness program that provides critical insights into how they can avoid these risks.

Here are five critical elements that ought to be part of any cybersecurity awareness program.

1. **Beware of public Wi-Fi**

While most public Wi-Fi access points are perfectly safe, that’s not always true. Criminals will often broadcast their device as a public access point, especially in public locations like food courts or at large events. Then, when a user connects to the internet through them, the criminal is able to intercept all the data moving between the victim and their online shopping site, bank, or wherever else they browse to.

Many smart devices will also automatically search for known connection points, like your home Wi-Fi. Newer attacks watch for this behaviour and simply ask the device what SSID they are looking for. When the phone tells them it is looking for its ‘home’ router, the attack replies with, *“I’m your home router,”* and the phone goes ahead and connects. Smart devices will do the same thing with Bluetooth connections, automatically connecting to available access points.

To combat these issues, it’s a good practice for users to turn off Wi-Fi and Bluetooth until they are needed. In the case of wireless access, they should verify the SSID of a location, often by simply asking an establishment for the name of their Wi-Fi access point before connecting. Users should also consider installing VPN software so they can ensure they only make secure, encrypted connections to known services.

2. Use better passwords

Another mistake users make is using the exact same password for all their online accounts, usually because remembering a unique password for each site they have an account on may be impossible. But if a criminal manages to intercept that password, they now have access to all of the user’s accounts, including banking and shopping sites.

The do's and don'ts of password management

Xneelo 19 Nov 2019

The best option is to use a password vault that stores the username and password for each account, so all that needs to be remembered is the password for the vault. Of course, extra care must be taken to ensure that the vault password is especially strong and easily remembered. One trick for creating strong passwords is to use the first letters of a sentence, song lyric, or phrase, insert capital letters, numbers, and special characters, and you’ve got a pretty secure password.

To be even more secure, consider adding two-factor authentication for any location where sensitive data is stored. It’s an extra step in the login process, but will significantly increase the security of their account and data.

3. Recognise phishing

You’ve probably repeated to your users to never click on links in advertisements sent to their email or posted on websites unless they check them first. There are a lot of tells, such as poor writing or grammar, complex or misspelled

URLs and poor layout that can be a key giveaway that an email is malicious.

But it turns out that there will always be someone who can’t resist opening an email, launching an attachment from someone they don’t know or clicking on a link on a website – especially when it includes an enticing subject line. Which is why any educational efforts need to be supplemented with effective Email Security Gateway and Web Application Firewall solutions that can detect spam and phishing, validate links, and run executable files in a sandbox – even for personal email – to ensure that malicious traps simply do not get through to an end-user.

4. **Update devices and use security software**

   Users should have a corporate-approved security agent or MDM solution installed on any device that has access to corporate resources. This software also needs to be kept updated, and device scans should be run regularly.

   Similarly, endpoint devices need to be regularly updated and patched. Network Access Controls should be able to detect whether security and OS software is current, and if not, users should be either redirected to a remediation server to perform necessary updates or alerted as to the unsecured status of their device.

5. **Monitor social media**

   Criminals will often personalise an attack to make it more likely that a victim will click on a link. And the most commonplace for them to get that personal information is from social media sites.

5 Common mistakes we all make on social media

18 Sep 2019

The easiest way to prevent that is to simply set up strict privacy controls that only allow pre-selected people to see your page. Individuals wanting an open social media profile need to carefully select who they will friend. If you don’t know someone, or if anything on their personal site seems odd, dismiss their request. And even if the person is someone you know, first check to see if he or she is already a friend. If so, there’s a significant possibility that their account has been hijacked or duplicated.

Keep training messages short, clear, and regular

It is essential that you develop a comprehensive and effective security strategy for your users who have personal endpoint devices connected to your network. But don’t make the mistake of burying them in information. Break information down into easily digestible chunks. Provide a daily security tip. Post messages around the company, such as in the hallways or break room. Get the executive team to mention it in staff meetings. And provide checks, such as your own phishing emails, to help identify users that might need additional attention.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...

For more, visit: https://www.bizcommunity.com