Tips to Stay Cell Phone Savvy

By Manon Jacob from isolved

Written on *March 28, 2024*

Now that the holiday season is over, people quite often let their guard down to the dangers of bad actors and scammers. Despite Apple's reputation for security, iPhones rank among the most frequently breached mobile devices globally. Gil Shwed, cybersecurity billionaire and founder of Check Point Software, recently warned that iPhones are not more secure than Android phones. Shweb recently told Forbes magazine, "the attack surface has greatly expanded. We have seen this huge surge in mobile and malicious apps."

As few as 1% of cell phones carry security software, but 46% of companies found themselves infected by a malicious app brought into their ecosystem on an employee's phone. At Check Point, Shweb enforces security software on employee cell phones. If an employee wants to access corporate email or the corporate systems, they must use Check Point's threat prevention on their mobile phones.

At many companies, cell phones are vital for multifactor authentication (MFA). If the employee's phone is hacked and they can no longer access their apps, they will not be able to use their corporate systems. The following is based on a true story that actually happened to a real employee. Some of the details and the name of the employee have been modified for confidentiality purposes:

Stanley Hunter in Sales recently sent an alarming message to his company's IT team. It said, "Help, my cell phone has been hacked. They also got into my bank account too and stole $10,000! I shut down my cell phone number. It is no longer in existence. This creates problems in accessing company apps because I can no longer authenticate. "

Six months earlier, Stanley downloaded TikTok on his cell phone. He later deleted it, but the risk could have remained dormant on his system. Stan thinks he downloaded malware from a scammer on TikTok posing as a legitimate source.

Tip #1: Avoid Dangerous Apps including TikTok.

It is critical that end users limit the number of apps that they download and they are knowledgeable about the risks of each app. TikTok's own privacy policy states that they collect an enormous amount of user information including biometric data, private messages on the app, social network contacts, user's phone book contacts, technical information, user preferences, Tik Tok allows its business partners to collect information on a user's online activities, and the list goes on.

Norton, the anti-virus company, recently warned about 3 Tik Tok scams to be aware of in 2024: Romance Scams, Fake giveaways, and Phishing scams. Click here for the full article: Norton warns about TikTok scams in 2024.

In the phishing scam, a criminal will try to gain access to private information by pretending to be a legitimate source. On the TikTok app, a scammer may direct message a user and get the victim to click on a malicious link. They could also ask for login credentials or credit card information.

Tip #2: Avoid "Stranger Danger" Text Messaging from new "Friends."

One of the latest cell phone scams is what appears to be the "honest wrong number" and the "luring in" technique used by scammers. Cybersecurity has seen a few of these reports. Here is a true story based on what actually happened (once again names and specific details have been disguised for confidentiality purposes). Denise in IT received this text message:

Scammer: Hey thanks for the gifts! (emojis) Let's get together this weekend for dinner.

Denise: You have the wrong number.

Scammer: Didn't you save me in your contacts? (attempting to make Denise think this is real and to guilt her into responding back)

Denise: Who do you think this is? (Denise is suspicious and at the same time curious)

Scammer: Isn't this Lucy?

Denise: Wrong number. No this isn't.

Scammer: Oh, thank you for being such a kind person. I am so embarrassed.

Denise: No worries.

Scammer: You are so kind and thoughtful. I am Olivia May. May I know your name?

Denise: Deletes message and blocks contact.

In this case, Denise suspected from the beginning that this was a scammer. She continued out of curiosity to see what would happen. She immediately deleted and blocked the number before it escalated.

In these cases, the scammer tries to “befriend” their victim and scam them out of money. They make up a sad story and try to get the victim to wire money. They also provide malicious links that can do enormous damage. These links can download malware and wreak havoc on the cell phone.

Tip #3. Use Cybersecurity Tools such as Antivirus software and Password Managers

Today almost everyone has antivirus software on their desktops and laptops, but they do not even consider their cell phones. Cell phones house a plethora of confidential information and they are used for banking, online shopping, and they are used for critical financial transactions. There are many antivirus tools for cell phones to explore. Bitdefender is considered to be one of the best and it is very light to use. It has robust malware scanning and it makes sure that you do not visit malware-infested sites even by mistake. Norton Mobile Security focuses on protection, security, identity, and privacy. It also has a built-in malware scanner that will notify you about threats and vulnerabilities on your phone.

Password managers keep all your passwords secure and in one place. For the iPhone, iCloud keychain keeps passwords updated across all your devices. For all users including Android, there is NordPass, Keeper, and 1Password among just a few of the options available.

Tip #4: Avoid Scanning QR Codes

Recently bad actors have started using QR codes as an attack vector. People are now scanning QR codes at restaurants and all over. Malicious URLs can easily be embedded into them. Just recently the FBI warned Americans about the dangers of using QR codes. Victims could end up giving attackers full access to their mobile devices. The bad actors in turn could gain access to user’s contacts, download malware, or send a person to a fake portal.

There are a few things you can do to stay safe and prepared:

1. Avoid QR codes whenever possible. Ask to see the hardcopy of the menu.
2. Use a scanner that directly displays the website after scanning the code.
3. Remain vigilant. If the QR code appears to be tampered with, trust your instincts, and say something. Remember, if something appears unusual, it might be. It is better to be safe.

If you suspect that your cell phone has been hacked, immediately contact your cell phone provider, and do not use your phone to access sensitive systems. Also, contact your company’s IT team. They may be helpful getting you set up again with multifactor authentication.