MOBILE CYBERSECURITY CHEAT SHEET

① Mobile Cybersecurity

Advancements in mobile technology have transformed every employee into a roaming cybersecurity vulnerability with vulnerability with many employees using their personal smartphones for work purposes. Small businesses beware! It might seem like a cost-effective solution for the business but it is not harmless. Keep in mind that these personal mobile devices are more powerful than some of desktop/laptop PCs being used today that are only three or four years old — and they're just as open to cyber intrusions by hackers. Being open to compromises means breaches and exposed data that can cost your company millions of dollars per incident. Anytime a smartphone or tablet connects to the open internet it presents a risk to your security. If that device has been infiltrated or hijacked and it has access to internal company resources can be accessed. These are the huge cybersecurity risks that your small business must be aware of.

② Common Mobile Threats

1. Physical Security - When you consider how easily these devices are transported they can be easily lost or stolen. Not only will you have costs related to the replacement of the device itself, but you must consider what type of data was on the device and the access the device had to your corporate systems.
2. Mobile Malware - Hackers are using specialized malware to target mobile devices. If an infected smartphone or tablet gets on your small business's network can lead to serious damage. Viruses can get mobile devices in a couple

Common Mobile Threats (con't.) ②

of different ways: rogue web pages or malicious native applications. Then there are native app viruses which are even more of a problem because of the access to the devices internal processes (data storage and memory.) These a nefarious applications when installed are capable of accessing private data or spying on your activities.
3. Responsive Malware - Responsive malware by makes its way into your system via traditional means like an SQL injection or cross-site scripting invasion of the site server and files. Customers using mobile-devices users will be viewing a responsive layout version of your website (ie.the display adapts to screen size.) Often times these will direct your mobile customers to a porn, gambling, or pharmaceutical sites. The best defense against these is to adhere to standard security recommendations which include keeping plugins, themes, and core code updated, using robust anti-virus and anti-malware protection, and hardening your login with strategies like Two-Factor Authentication and restricted login attempts.

Continue reading on next page >

MOBILE CYBERSECURITY CHEAT SHEET

② Common Mobile Threats (con't.)

4. Public network threats - public wi-fi networks are a common target for attack because people tend to be unaware of the the potential risks to data that public networks pose.
5. IoT-related threats - There are a diverse number of mobile devices due to the world of the Internet of Things (IoT). Connected IoT devices can include everything from coffee makers, activity trackers, smart speakers and smart watches, that feature wi-fi technology. When these types of devices installed in your office, be aware that they are vulnerable to attack just as much as smartphones and tablets.

③ Solutions to Mobile Cybersecurity

1. Security Codes - Before distributing a mobile device to any employee be sure to add a complex security code for unlocking the mobile device. I do not recommend using biometric for unlocking the screen. Save biometrics for opening applications when the phone is unlocked. That way if a criminal manages to get access to the phone or tablet, they will not be able to access the content inside it.
2. Remote Access Management - Many small businesses opt to use a bring your own device (BYOD) system for mobile devices.

Solutions to Mobile Cybersecurity (con't.) ③

They think that it will reduce the financial impact of supporting mobile platforms allowing employees to manage a single set of devices for home and work. There is a significant drawback as individuals will be using their private devices to access corporate email, chat, and file systems, so it is essential that precautions be put into place. There are remote access management tools available for both the iOS and Android operating systems. These allow IT administrators to interact with any devices on their network. However as with any policy, there is a downside. In the case of a BYOD policy, it requires that employees give up some privacy to ensure the company's security. You can assure your employees that these mobile device management tools are not designed to spy on individual people but to provide a mechanism for administrators to either enable or disable access to internal resources. Should a device be lost or stolen, administrators can remotely wipe all of its content to protect confidential company information.
3. Virtual Private Network (VPN) - A VPN encrypts an online session between the device and the open internet. Once a VPN connection is activated on your smartphone or tablet, the device will be assigned a new IP address and all outgoing traffic will be routed through the VPN. Many small businesses are choosing to enforce

Continue reading on next page >

MOBILE CYBERSECURITY CHEAT SHEET

(CONTINUED)

③ Solutions to Mobile Cybersecurity (con't.)

a strict VPN policy for employees who work remotely or use a mobile device to access corporate resources such as email. The benefit of a VPN is that even if a hacker were to intercept your web traffic, they would not be able to steal the data because it is encrypted.
4. Domain Name Management - To stay updated and secure, your domain needs ongoing management. The domain name owner needs to practice some form of domain management—and a wide range of domain management services and tools can help users with tasks ranging from keeping domains updated and secure to tracking performance with sophisticated analytics. These tools allow a domain owner to perform essential tasks such as renewing or terminating domain name registration, determining name servers and hosting providers, and making changes to domain names.

Concluding Thoughts ④

Mobile security can be a significant challenge for small business owners as they may not have the resources or budget to make a significant investment in cybersecurity. The options listed above will not break the bank. However, the small financial investment you make will protect you for a lot loss than what you will end up paying if a hacker breaches your system and steals your business's information. If you choose to ignore mobile security you could pay a much steeper price in loss of profits and reputation..

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH