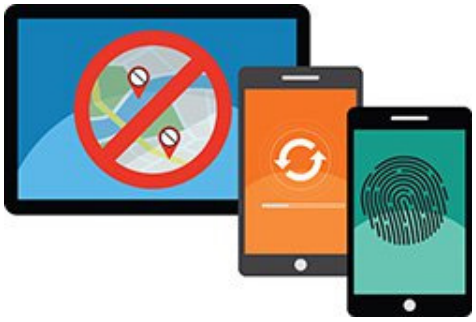
BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
September 2019

Securing Your Mobile Devices



Your mobile devices are an amazing and easy way to communicate with friends, shop or bank online, watch movies, play games, and perform a myriad of other activities. Since your devices are such an important part of your life, here are some simple steps to keep you and your devices safe and secure.

Securing Your Devices

It may surprise you to know that the biggest risk to your mobile device is not hackers, but most likely you. You are far more likely to lose or forget a mobile device then have someone hack into it. The number one thing you should do to protect your devices is enable automatic locking of the screen, often called a screen lock. This means every time you want to use your device you first have to unlock the screen, such as with a strong passcode or your fingerprint. This helps ensure that no one can access your device if it is lost or stolen. Here are several more tips to help protect your devices:

Updating

Enable automatic updating on your devices so they are always running the latest version of the operating system and apps. Attackers are always looking for new weaknesses in software, and vendors are constantly releasing new updates and patches to them. By always running the latest operating system and mobile apps, you make it much harder for anyone to hack into your devices.

Tracking

Install or enable software to remotely track your mobile device over the Internet. This way, if your device is lost or stolen, you can connect to it over the Internet and find its location, or in a worst-case situation, remotely wipe all of your information on it.

Trusted Apps

Only download apps you need and from trusted sources. For iPads or iPhones, that means download apps from the Apple App Store. For Android, download apps from Google Play; for Amazon tablets, stick with the Amazon App Store. While you may be able to download apps from other sites, these are not vetted and are far more likely to be infected. Also, before downloading an app, check to make sure it has lots of positive reviews and is actively updated by the vendor. Stay away from brand new apps, apps with few reviews, or ones that are rarely updated. Finally, regardless of where you got your app, once you no longer need or actively use the app, we recommend you delete it from your device.

Privacy Options

When installing a new app, make sure you review the privacy options. For example, does the app you just downloaded really need to have access to all your friends' and contacts' information? We also recommend you disable location tracking for everything, then enable location for only the apps you feel need it. If you are uncomfortable

(Continued on next page)

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

Securing Devices (Cont.)

with the permission requirements of an app, find a different one that meets your needs. In addition, periodically check the permissions to ensure they have not changed.

Backups

Always back up your data. For mobile devices, a great deal of your information is often backed up automatically, such as your photos or messages. However, backups also store your configurations, apps, and other device information, making it much easier to recover from a lost device or transition to a new one.

Work

When at work, be extra careful and never take any pictures or video that may accidentally include sensitive information, such as pictures of whiteboards or computer screens.

Your mobile devices are a powerful tool, one that we want you to enjoy and use. Just following these few simple steps can go a long way to keeping you and your devices secure.

Ransomware Now Sends Malicious Texts Through Mobile Device

If you own an Android device, there's a new threat to be at least moderately concerned about. It takes the form of a new ransomware family that spreads from one victim to the next with text messages that contain poisoned links to every contact on an infected device.

The ESET research team that found the software had this to say about it:

"Due to narrow targeting and flaws in both execution of the campaign and implementation of its encryption, the impact of this new ransomware is limited.

If your system is infected, the first thing it will do is raid your contacts list and send SMS text messages to everyone on it. Anybody who clicks on the link in the SMS message will also be infected.

After sending a flurry of messages, the malware will turn its attention to your device itself. It will then set about the task of encrypting most of the files on your device. Fortunately, the people behind this new threat prove themselves to be new to the game."

ESET continues:

"After the ransomware sends out this batch of malicious SMSes, it encrypts most user files on the device and requests a ransom. Due to flawed encryption, it is possible to decrypt the affected files without any assistance from the attacker."

All in all, this issue is only of minor concern. It's annoying, and certainly time consuming to restore your files. However, it's not an especially dangerous malware strain - yet, and that's the problem.

Whomever is behind this new threat certainly has the right idea, even if they lack the technical chops to pull it off. Skills, however, can be learned and honed. As a first try, this effort is disturbing because it's clever. The moment the people who wrote the code get the technical skills to pair with that cleverness, they're going to be genuinely dangerous.

September 2, 1666
The Great Fire of London was started, completely destroying the old city located within the ancient Roman Walls. It was believed to have started in a bakery and took three days to put out.

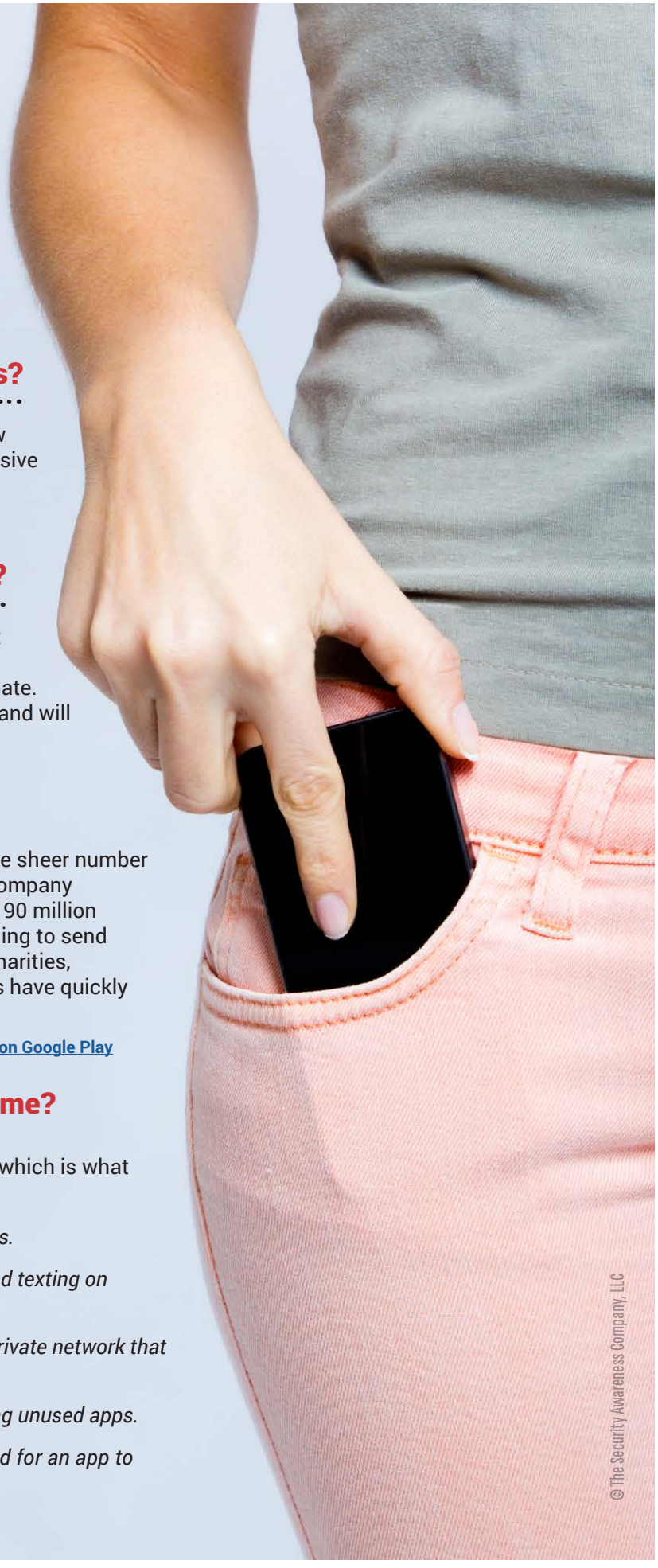
September 5, 1774
The 1st Continental Congress was called to order. Comprised of delegates from all 13 American colonies, it served as the governing body during the American Revolution, from 1774 to 1789. Two years later, on September 9, it changed the name of the United Colonies to the United States.

September 5th, 1961
President John F. Kennedy signed a hijacking bill, making air piracy a federal crime. Punishment ranged from a $10,000 fine to 20 years in prison; if a deadly weapon was used, the perpetrator(s) could receive life in prison or even death.

September 8, 1974
President Gerald Ford gave an unconditional pardon to former president Richard M. Nixon, for his role in the infamous "Watergate" fiasco.

September 9, 2006
Typhoon Ketsana hit the Philippines, China, Vietnam, Cambodia, Laos, and Thailand, resulting in 750 fatalities and over $1.09 billion in damages.

The Threat in Your Pocket



Why do cybercriminals target smartphones?

The obvious answer: there are a lot of them. Estimates show that over 5.1 billion people own a smartphone. That's a massive target oozing with hacking potential.

Source: BankMyCell.com Blog - How Many Phones Are In The World?

What makes mobile devices so vulnerable?

Smartphones have screen-size limitations that restrict what can be viewed. For example, it's difficult to hover over links to show their full URL or to ensure that a webpage is legitimate. Also, people are easily distracted when using smartphones and will often click quickly, without much thought.

How common are mobile attacks?

App stores struggle to catch malicious developers due to the sheer number of new apps uploaded every day. Not long ago, a research company identified six malicious applications which already had over 90 million downloads. Furthermore, cybercriminals utilize text messaging to send malicious links while impersonating financial institutions, charities, government agencies, utility companies, etc. Mobile devices have quickly become one of the top attack vectors for cybercriminals.

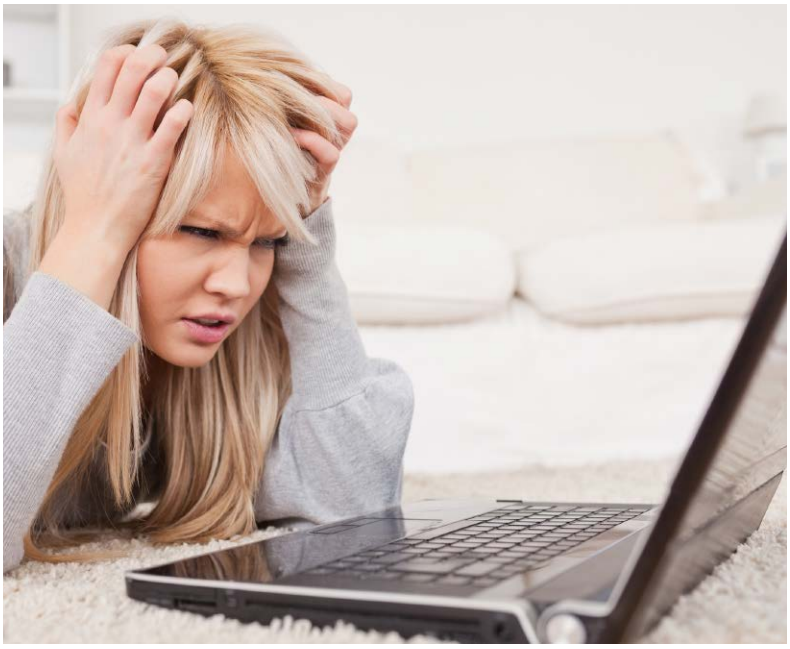
Source: Checkpoint Research Article - PreAMo: A Clicker Campaign found on Google Play

What can we do to prevent mobile cybercrime?

First and foremost, treat your smart device like a computer, which is what it is. That means you need to be:

- *Utilizing antivirus software and enabling automatic updates.*
- *Staying alert for phishing attacks, which come via email and texting on smartphones.*
- *Never connecting to public WiFi without a VPN—a virtual private network that encrypts your connection.*
- *Vetting all apps before downloading AND regularly removing unused apps.*
- *Allowing only the minimum number of permissions needed for an app to properly function.*
- *Always following our organization's mobile device policies.*

BIZ NET BUSINESS - NETWORKS Protecting Your Business With Care For Your IT Services



The Personal Impact of Cybercrime

When an organization suffers a data breach, the net results can cost millions, while permanently damaging relationships with our clients and customers. That's a big part of why we take our security policies and awareness training so seriously.

But we take the ***personal impact*** of data breaches just as seriously, because at the end of the day, we are all subject to having our personal data compromised. Here are a few examples of cybercrime that impact each of us on a personal level, and what you can do to prevent it.

Identity Theft

Perhaps the most immediate threat in all cases, identity theft allows cybercriminals to open accounts, make purchases, or even file tax returns in your name, among other things. ***One way to avoid this is to limit the amount of personal data you make public.*** Also, know that government entities won't email you asking for payments or sensitive info. Consider placing fraud alerts or freezes on your credit reports.

Phishing

Cybercriminals use phishing attacks to execute a wide range of malicious intentions, from stealing data to obstructing operations. Stay alert for any messages that contain awkward or poor grammar, threatening language, or random links. ***Remain highly skeptical of any requests for sensitive info.***

Ransomware

A form of malware that encrypts files and systems until a ransom has been paid, ransomware yields scary results, such as when hospitals are unable to access databases or cities are unable to render public services. But criminals will happily target individuals, as well. Don't fall victim. ***Think before you click,*** and never download random attachments in emails.

DDoS Attacks

Short for distributed denial-of-service, criminals use DDoS attacks to shut down websites and knock all internet services offline, usually impacting millions of people. DDoS is made possible by smart devices left unprotected. That's why it's imperative that you ***update default usernames and passwords of connected devices*** ASAP, and enable auto-update of apps and smart devices wherever possible.

Vishing

Short for voice phishing, vishing attackers utilize telephone services to trick victims into divulging financial or other forms of private data. Just like with phishing, we need to treat random requests for data with a high degree of skepticism. ***Never assume someone is who they say they are,*** and don't blindly trust a caller ID, since cybercriminals figured out how to spoof those years ago.

Remember, preventing cybercrime starts with common sense and ends with following our organization's policies. If you ever have questions about our security efforts, please don't hesitate to ask.