Welcome to the Gemini IBD ® Cybersecurity Infographics Newsletter

4TH EDITION, VOLUME 1
DECEMBER 13, 2018

We all know that the Smartphone today has become an extension of both our personal and professional lives. We simply cannot live without it. We use it for our primary means of communications with friends, family, and co-workers. We share messages, pictures, videos, work related documents, etc. But, just for a minute think about this dreadful scenario:

Suppose that your Smartphone is lost or stolen, or even hit by a Cyber attack? What would you do? The first feeling we will have is that of sheer panic and paralysis until our rational side can kick in. Believe it or not, the Smartphone is actually one of the prime targets for the Cyber attacker. The goal of this newsletter is to provide some detail into what some of the top Cyber threats are to the Smartphone, and the steps that you can do protect it.

How Much We Are Addicted to Our Smartphone

- 12% of all adults use their Smartphone in the shower;
- 56% of all users check their Smartphone one last time before they go to bed;
- 75% of all users check their Smartphone when they first wake up from sleep;
- 50% of users have a feeling of paralysis when they are on the go and leave their Smartphone at home;
- 26% of all car accidents are caused by driver inattentivness because they are using their Smartphone behind the wheel;
- 75% of Smartphone users have admitted to texting while they are actually driving (this is now against the law, and one can face huge penalties for this);

- 40% of users play with their Smartphone while they are on the toilet;
- 20% of adults in the age bracket between 18-35 have used their Smartphone while they have engaged in sexual intercourse with their partner;
- 61% of users sleep with the Smartphone under their pillow;
- 44% of users check their Smartphone on daily basis when they are on vacation;
- 56% of adult parents check their Smartphone while they are taking their kids to school or other activities;
- 77% of adults and teenagers are always arguing about Smartphone usage – more so than school work or grades.
- People touch their Smartphones at least 2,617 times per day. Top 10% of users touch their Smartphones 5,247 times per day, which translates into over 1,000,000 touches per year and 3 hours of phone screen usage on a daily basis.

- iPhone users check their devices 80 times per day, and Android users check their devices 110 times per day, which translates into iPhone users checking their phones 6-7 times per every hour, or once every 10 minutes.
- Smartphone users surf the Web for at least 5 hours per day.
- Users spend on average 3 hours 23 minutes per day using mobile apps;
- Users will download 268 million mobile apps in 2018.
- Mobile app usage constitutes 70% of all Smartphone activity.
- 88% of users who search for a product or service from a local store will visit that brick and mortar location within 24 hours.
- 58% of all Google searches originate from a Smartphone device.
- 75% of Facebook videos are viewed from the Smartphone.
- 68% of all E-Mails are first opened up on a Smartphone.

- Video makes up 69% of all Smartphone consumption by users.
- 71% of all users use their Smartphone for all kinds and types of Internet usage.
- 1.2 Billion people, or 20% of the world's population owns a Smartphone.
- 80% of the American population owns a Smartphone.
- 51% of users use their Smartphone for online shopping purposes.
- Users send an average of 110 text messages from just one Smartphone on a daily basis.
- 42% of users use their Smartphone for entertainment purposes, rather than going out, spending time with family or significant other, etc.
- Users spend 90+ hours a month on their Smartphone (this is 1,100 hours per year).
- 85% of American users use their Smartphone for catching up on the news headlines.
- In the United States, there are at least 350,000,000 Smartphone users (this is actually even more than the American population itself, which stands at 325.7 Million people).
- Finally, 30% of users would rather giving up being intimate with their partner than give up their Smartphone.

The Top Cyber Threats to the Smartphone In 2018

As mentioned, the Smartphone is fast becoming the target for Cyber attackers these days. Really, in today's times, anything can be a prime target, but the Cyber attacker knows that once our Smartphone is hijacked or compromised, and literally "locked up" because of an attack, a horrible feeling of paralysis will set in just a matter of seconds. True, we can always go back to the vendor from which we initially purchased our Smartphone from, and simply restore everything from a cloud-based backup (such as the iCloud – and this is assuming that you have actually done this), but is this feeling of hopelessness that the Cyber attacker is preying upon.

For example, during these few hours while you are desperately trying to figure out what to do, the Cyber attacker can literally steal all of your personal and confidential information and data in just a matter of minutes.

But to do this, the Cyber attacker first has to create a sophisticated attack of sorts, or take advantage of the flaws in the hardware device of the Smartphone itself, or in the Operating System, or even in the patches and upgrades that have been installed onto it. In fact:

- There are 3.5 million pieces of malware for just 1 million devices here in the United States. These means that for 1 Smartphone, there are 3 pieces of malware that can be installed onto it-a huge security threat!!!
- There are over 230,000 new pieces of malware code that come out every day!!!

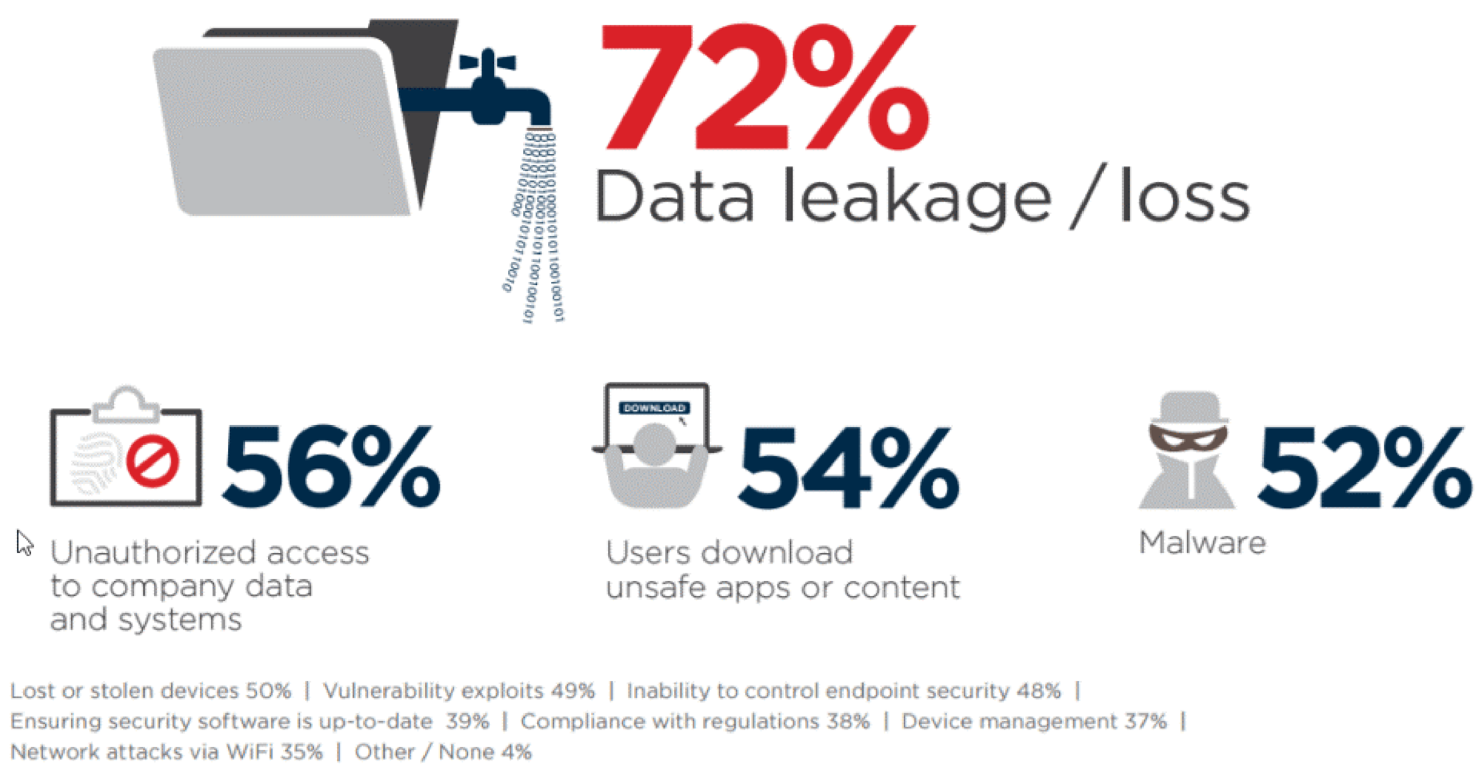
In this regard, here are the top 5 Cyber threats to Smartphones that you need to be aware of. This is how the Cyber attacker can come not only after you, but even society as a whole and perhaps even cause mass hysteria as a result.

Data Leakage

This is not a direct attack by a Cyber attacker per se, but rather it is a flaw in the mobile app itself. Other than communicating with one another, we also use our Smartphone extensively in order to download mobile apps. These are small software packages which can be downloaded from either the Apple Store or Google Play.

In these instances, the top threat for Smartphones is what is known specifically as "Riskware". These are mobile apps which are free to download, and it usually has been advertised somewhere on a mobile ad. But, the customer does not know that these kinds of mobile apps have actually not been tested for any kind of security. Apple and Google usually scrutinize every mobile app they receive from software developers before they are uploaded onto their respective stores.

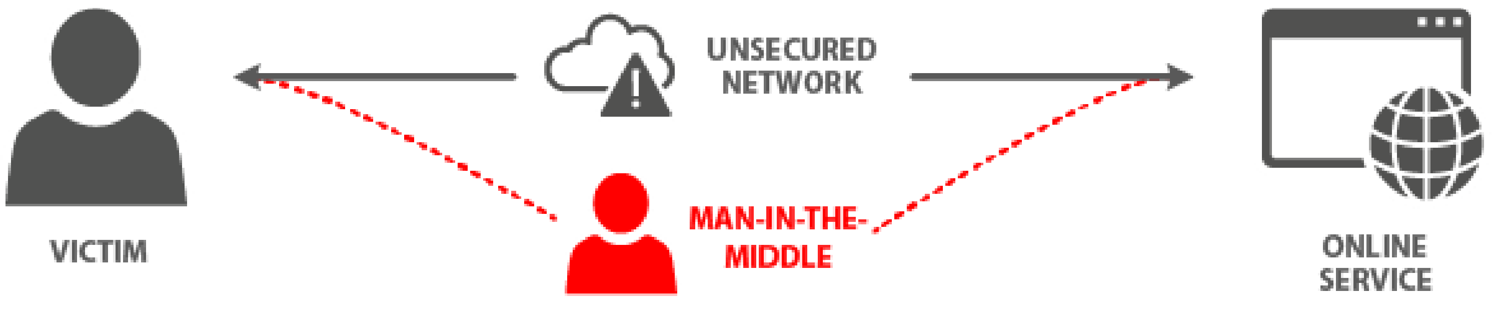
Q: What are your main security concerns related to BYOD?



Because these free apps have not been tested, they very often contain malicious code which makes its way into the Smartphone of the customer, and from there, the Cyber attacker can then get to all the stuff they want to in order to launch an Identity Theft attack, without you even realizing it. For example, " . . . these free apps perform as advertised, but also send personal—and potentially corporate—data to a remote server, where it is mined by advertisers or even cybercriminals." (SOURCE: 1).

Unsecured WiFi Spots

When we initially purchase our Smartphone, we normally get a certain amount of data in our plan. This simply means that we have an assigned number of Gigabits of data we can use to access the Internet before we have to pay any overage charges if we go over.



By intercepting communication through an unsecured network, the attacker can steal all kinds of information in real time.

Most customers consume 12 Gigabytes each month. That is a lot of data! Truth be told, just as much as our Smartphone is our most prized possession, second in line from that is the data plan that we have it. It can likened to that of fuel which drives our Smartphone consumption, and of course, wherever we at, we always want to try to conserve the amount of data so that we do not go over and pay extra.

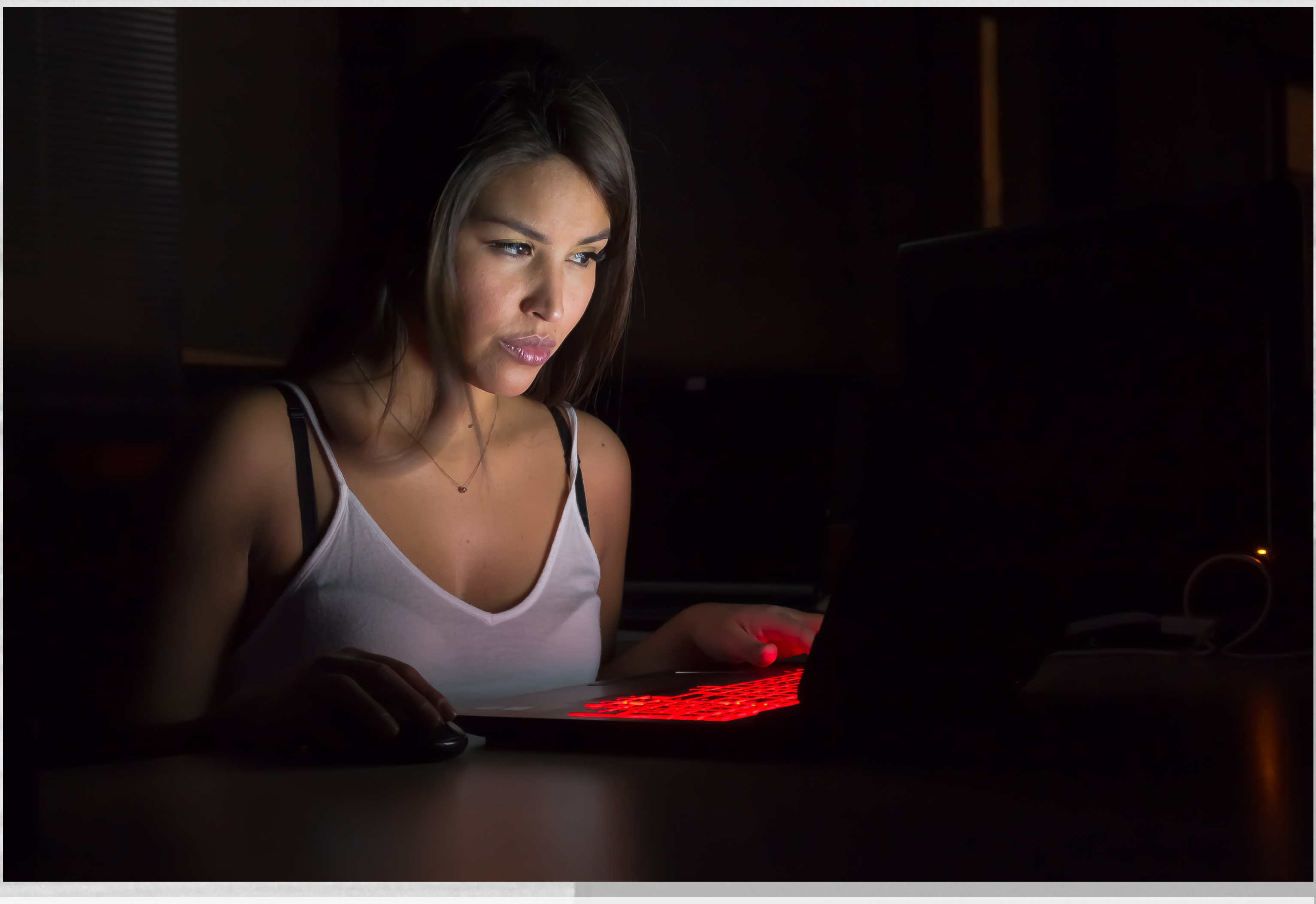
So as a result, whenever we can, we always try to make use of free data whenever and wherever it is possible, such as that in a pubic place like Starbuck's or Panera Bread. These places provide what is known as a "WiFi Hotspot".

The Cyber attacker is fully aware of this approach in human thinking (which is actually a huge vulnerability), and thus this is where they try to capture the actual transmission of information and data from your Smartphone to the free data "Hotspot" at the public location. Believe it or not this line of communications is not secure by any means, so it is very easy for the Cyber attacker to easily capture your passwords and financial account information (such as credit card numbers, etc). These are also known technically as "Man In The Middle Attacks", because the Cyber attacker is literally in between the line of unsecured communications between your Smartphone, and the public WiFi Hotspot.

Network Spoofing

This security vulnerability posed to Smartphones goes back to the previous example of the public WiFi Hotpsots that are found in the public places (once again like Starbuck's or Panera Bread). Before you can actually gain access to the free data connection, you have to login with the username and password that is given (which is also publicly available), and agree to their terms of usage. Usually this is an entire webpage, and there is no way to prove its authenticity. For the most part, these websites are actually legitimate, but given the level of the sophistication of the Cyber attacker these days, a spoofed up web page can be designed and replaced quite easily.

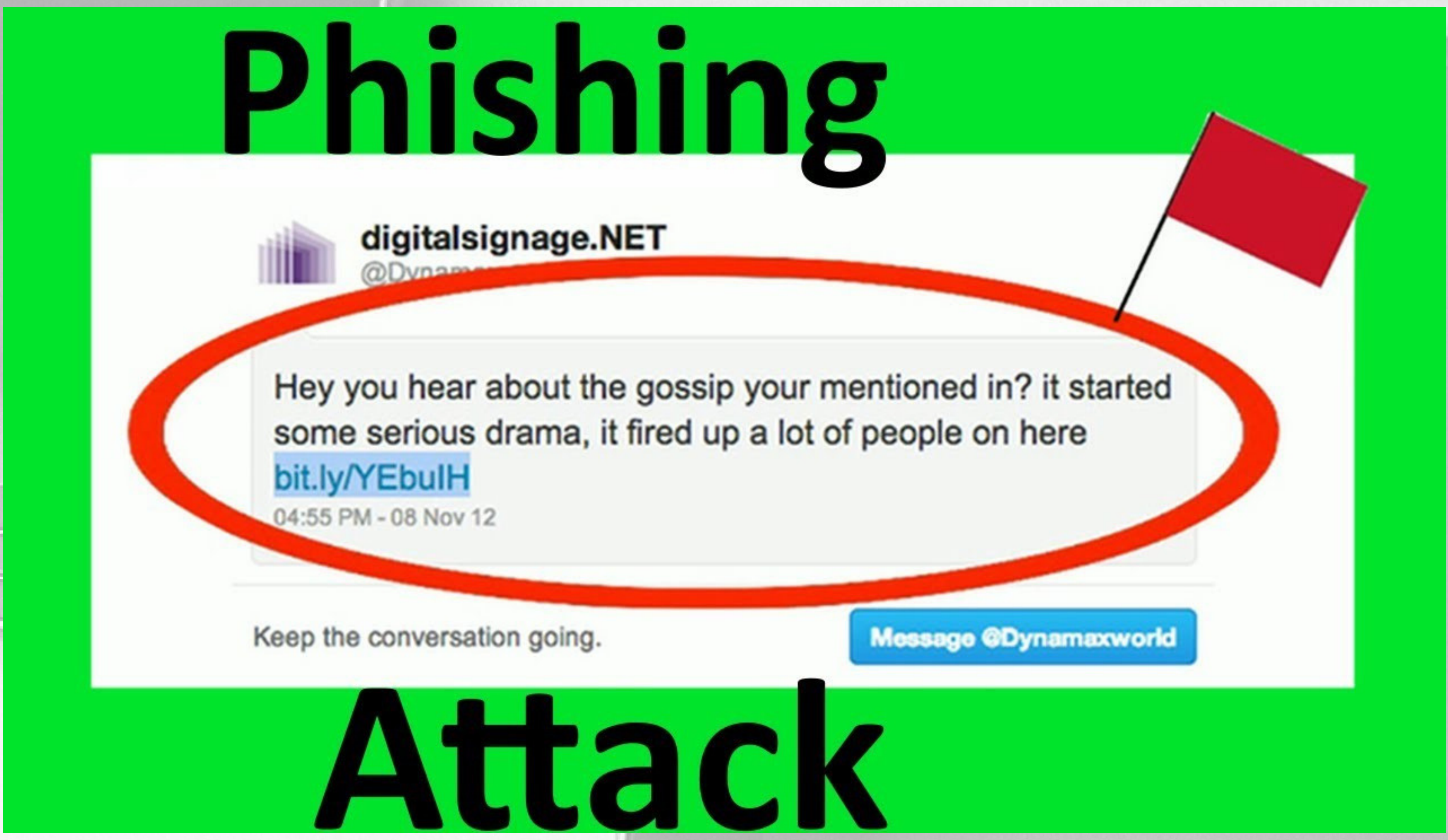
Typically, the Cyber attacker names these spoofed public WiFi Hotspots such as "Airport Wi-Fi" or even "Coffeehouse WiFi". Unlike the legitimate login pages, the customer actually has to create an account in order to gain access the supposedly free data connection. But, given how much people hate remembering hundreds of passwords, we tend to use the same username/password combination for just about everything we login into. The Cyber attacker is also fully aware of this, and after you have created this account and logged in, and also in a manner very similar to that of a Man In The Middle Attack, the Cyber attacker will see the websites you are accessing. If anything looks private and confidential, they will then later on use that same username/password combination that you have created, login, and covertly hijack everything and anything that they can.



Phishing Attacks

This is a type of Social Engineering attack, and although it is has been around for a long time, it is still widely used by the Cyber attacker of today, especially those on Smartphones. Phishing can be defined as follows:

> "It is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as . . . banking and credit card details and passwords". (SOURCE: 2).



digitalsignage.NET
@Dynam...

Hey you hear about the gossip your mentioned in? it started some serious drama, it fired up a lot of people on here bit.ly/YEbulH

04:55 PM - 08 Nov 12

Keep the conversation going.

The telltale signs of a Phishing attack include the following:

- The content of the E-Mail message has poor spelling or grammar: Phishing E-Mails often contain misspelled words, or even extra digits in the telephone number in the signatory component of the message. At first glance, these can be very difficult to find, but after a second or third look, they can be spotted. For instance, a phony message would contain the salutary line of "Dear eBay Costumer" instead of "Dear eBay Customer". Also, look in the subject line as well for any misspellings. Most e-mail applications are good in catching this, but some still fall through the cracks and make their way into your inbox.
- The hyperlinked URL is different that the one that is presented: Most Phishing E-Mail messages contain the name of a legitimate organization, but with a phony URL that is hyperlinked to it. For example, you could get what looks like a legitimate E-Mail message from PayPal, and towards the end of the message, it will say something like: "Check your PayPal account here." Obviously, the name looks authentic enough, but instead of taking you to www.paypal.com, the hyperlink displays a different URL (hover over it to see it).
- The E-Mail message has a sense of urgency to it: The content of a Phishing E-Mail will often have a strong sense of action to take. For example, it may say that your PayPal account has been closed, put on hold, or that there is even some sort of fraudulent activity that has occurred on it. In these instances, there will also be a link to take you to your account, but once again, it will be a phony one.
- It will contain a suspicious attachment: Most legitimate business entities or even individuals will not send you an attachment unless you have specifically requested one. Sometimes, Phishing E-Mails will contain an attachment, which will very often be in a .DOC or .XLS file extension. It will look like that these attachments are coming from somebody you know. These attachments contain a malware or a spyware executable program which will launch onto your computer or wireless device once they are downloaded and opened.

Ransomware

In this kind of Cyber attack, Cyber attackers want to hold your Smartphone hostage until you literally pay a ransom payment. This kind of attack is known as "Ransomware", and it can further elaborated on as follows:

"It is a type of malware that prevents or limits a user's access to their computer system, either by locking the system's screen or by locking the user's files unless a ransom is paid." (SOURCE: 3).

There are three types of Ransomware attacks:

- Scareware:

As the name implies, this kind of attack is just merely designed to scare or frighten you. These kinds of attacks primarily make use of annoying pop messages. One of the most "famous" of these is the pop up which claims that some sort of malware has been detected on your computer, and in order to get rid of it, you have to pay a small ransom. You will know if you if you have been hit by this kind of Ransomware attack if these pop ups keep constantly appearing. The only way to get rid of it is to install anti-malware software, such as the ones available from Norton and Kaspersky.

- Screen Lockers:

This is the next step up in terms of the severity level of Ransomware attacks. With this, your computer screen locks up, and as a result, you are completely frozen from accessing your files and folders. To make matters even worse, the message that appears will typically have an FBI, Secret Service, or a Department of Justice official seal, in order to make it look like that you have been caught doing some sort of illicit activity online. In order to unfreeze your screen, there will also be a message that you have pay a rather hefty fine. But keep in mind that these government agencies would never ask you to pay up. Probably the best way to get your screen unlocked is to take it to a local Geek Squad to clean your computer of the Ransomware. If this doesn't work, you may then have to get a new computer all together.

- Encrypting Ransomware:

These are deemed to be the worst kind of attack. In these particular instances, the Cyber attacker will steal your files, and encrypt them with a very complex mathematical algorithm, which will be very difficult to crack. In order to get your files back, the Cyber attacker will demand a large amount of money, to be paid by Bitcoin. Once they get this money, they claim that they will send to you the decryption key in order to not only retrieve your files, but to unscramble them as well into a decipherable state (in other words, making them like they were before they were hijacked). But most often this never happens, because once you pay up, the Cyber attacker often disappears. Since you have paid with a virtual currency, there is no way of tracking them down either (unlike paper currency, where you can use marked bills for these purposes).

How to Protect Your Smartphone

Given how much that we are addicted to our Smartphones and how much they are prone to Cyber attacks, the next question to be asked is "How Do I Protect My Smartphone?"

A simple Google search will reveal a plethora of ways to do this, but it all comes down to two things:

- Keeping your Smartphone updated with the latest Operating Systems, Software patches and upgrades;
- Using common sense and trusting your gut when something does not feel right.

Just know that you have options available to you that will keep you safe. Here at BN.net, we have several tips to help keep your Smartphone safe and secure.

Option One: Use Two Factor Authentication. This is also known as “2FA” for short. Essentially this means that you are using two layers of security to protect your Smartphone. The first one is in creating a strong password or PIN Number when you first log in. Obviously, you need to create it so that it is complex enough to be cracked, but also created in a way that you can remember it easily. There are many suggestions how to create strong passwords for both Android and iPhone devices, but here are two reputable sources that you should consider looking further into.

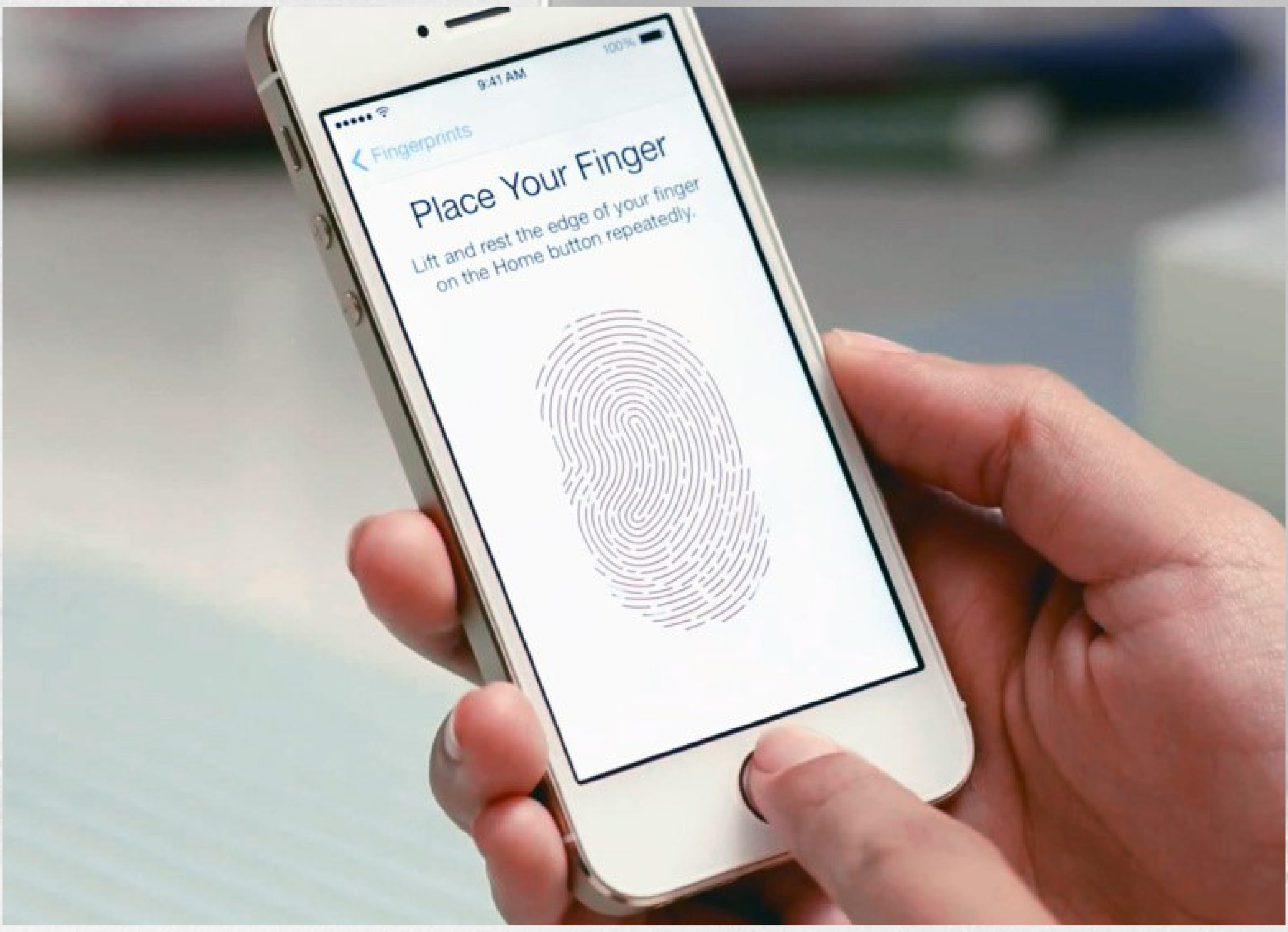
iPhone

CLICK HERE

Android

The second layer of security makes use of what is known as “Biometrics”. This is just another way of confirming your identity based upon your unique, physiological characteristics. Apple has made use of this, both from the standpoint of Fingerprint and Facial Recognition. These are known as “TouchID”, and “FaceID”, respectively.

TouchID illustrates this concept.


9:41 AM
100%
Fingerprints
Place Your Finger
Lift and rest the edge of your finger on the Home button repeatedly.

FaceID, available on the iPhone X, illustrates this as well.

9:41
Back
Move your head slowly to complete the circle.
Accessibility Options
How To Make Face ID Work Faster On
iPhone X
SYSTWEAK

Option two: download only those mobile apps from trusted sources. By this, we mean only download the mobile apps that you need from the Apple Store, Google Play, The Amazon AppStore, and the Windows Store from Microsoft. Of course, there are no 100% guarantees here either, but at least these vendors carefully scrutinize the apps first before they are uploaded onto their respective sites. Never, ever download a mobile from a site that does authentic!!! Also, read reviews of the mobile app before your download them, and be careful about those apps which get control over Smartphone (such as the GPS tracking ones).

Option three: Stop online advertisers from tracking your movements. In order to avoid this from happening, never click on those pop up ads which appear when you a visit a particular website. For details on how to avoid this from happening to you, click here.

Option four: make sure that your Smartphone has the Remote Wipe Function, and it is enabled. As mentioned, the greatest feeling of paralysis will set if we ever lose our Smartphone or it gets stolen. True, we can always get a new one, but the next major concern is that information and data which resides on it will fall into the wrong hands. The good news is that a majority of the Smartphones now have what is known as the "Remote Wipe". By initiating this command, all of the information and data will be permanently in just a matter of a few seconds. However, the major brands have different ways of specifically configuring this, so:

iPhone

« CLICK HERE »

Android

In fact, there are even tracking based mobile apps that will allow to you track your lost or stolen Smartphone (but once again, only download the legitimate ones!!!)

Option five: make sure that the Public WiFi you use is legitimate. If you ever happen to find yourself at Starbuck's or Panera Bread (or for that matter, any public place that offers free WiFi), make sure that you are logging into a legitimate website. This is not always easy to do of course, so if you have any doubts whatsoever, always reach out to the manager of the public place that you are visiting and have them look at what you are logging into to make sure that it is authentic and real. For more tips on how to stay secure and safe when using a Public WiFi network, click here.

Option six: wipe your Smartphone clean before you get rid of it. We are always enticed to upgrade our current version of the Smartphone to the next one when our contracts are up. But before you give up your old phone, make sure that all of your personal information and data is completely wiped off. This simply does not mean just deleting the files, but actually going into the internal memory of the Smartphone and deleting it from there. There is always this false sense of security that simply a file is deleted, it is completely erased from the Smartphone. The truth is that it is not!!! The Cyber attacker can always use forensics based tools to get this and use it for malicious purposes. Click here for more information on how to wipe your Smartphone clean.

Option seven - the oldest and best mantra of all: always keep your Smartphone updated with the latest iOS, Windows Mobile OS, or the Android OS. This includes all of the relevant patches and software upgrades as well. True, this can take quite a bit of time, but at least you will be doing everything that you can to help protect your prized possession.

Thank you for reading our newsletter! If you have any questions, please contact us here at BN.Net, Inc.!!! At BN.Net, Inc. (TM), we also offer an array of Biometric products that can be used to help protect your wireless device. Click here to find out more

Sources:

1) https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threatsmart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

2) www.phishing.org

3) https://www.trendmicro.com/vinfo/us/security/definition/ransomware

4) http://www.dailyinfographic.com/15-terrifying-statistics-about-cell-phone-addiction

5) https://online.king.edu/news/cell-phone-addiction/

6) https://www.enolalabs.com/blog/archives/13-mobile-device-usage-stats-in-2017

7) https://searchengineland.com/report-nearly-60-percent-searches-now-mobile-devices-255025

8) https://blog.ezoic.com/mobile-usage-statistics-key-facts-and-findings-for-publishers/

9) https://hostadvice.com/blog/mobile-usage-facts-figures/

10) http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/

11) https://www.elephantjournal.com/2017/08/cell-phone-addiction-in-teens-is-real-scary-statistics-some-helpful-advice/

12) https://www.nbcnews.com/technology/8-10-americans-depend-cellphones-121536

13) https://www.mobilexco.com/blog/18-stats-to-help-you-plan-your-mobile-marketing-strategy-in-2018

14) https://expandedramblings.com/index.php/smartphone-statistics/

15) https://expandedramblings.com/index.php/smartphone-statistics/

16) https://www.addictiontips.net/phone-addiction/phone-addiction-facts/

17) https://www.nerdwallet.com/blog/utilities/how-much-data-do-you-need/

18) http://time.com/money/3920131/cellular-data/

19) https://www.komando.com/tips/12080/make-a-more-secure-passcode-for-ios

20) https://www.komando.com/tips/12053/protect-your-privacy-against-online-advertisers/all

21) https://www.komando.com/apps/2756/find-your-lost-iphone-or-ipad

22) https://www.komando.com/tips/363741/how-to-stay-safe-on-public-wi-fi-2/all

23) https://www.komando.com/tips/383734/one-thing-you-need-to-do-before-getting-rid-of-an-old-gadget-or-computer/all