BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
January 2019

What It Means To Be Mobile

When cell phones first hit the market, the term 'mobile' meant, quite literally, the ability to make and receive calls while on-the-go. Nothing more, nothing less. **But today, mobile means smart and connected.**

Placing and receiving phone calls aside, you can tell your smartwatch to add items to your grocery list while you order a pizza via an assistant such as the Amazon Echo or Google Home. While traveling, you can adjust the lights and temperature of your house with the touch of a button. When you get home, a smart camera recognizes your face and automatically unlocks the door for you.

The world of mobile now includes a massive web of connected devices (the Internet of Things, or IoT). It isn't just about having access while on-the-go. **It's about having control of nearly everything**, simply by accessing that convenient little smart device tucked in your pocket or strapped to your wrist.

Unfortunately, lost in this world of smart connections is the prioritization of security. **New technology rarely gets built with personal security in mind.** In fact, the market has become so saturated that manufacturers feel pressured to rush products out without adequately testing their resilience against cybercrime. As a result, end-users must thoroughly research IoT products *before* buying, and then somehow ensure that security settings are enabled to the max on all those devices they *do* purchase.

Here at work, always follow our organization's mobile policies. Whether bringing your own device or using one we've issued to you, **it's your job to know what is and what isn't allowed** with smart devices. If you need more information, please ask!

The Concerns of IoT

The 2016 Mirai botnet attack, which utilized **300,000 hacked smart devices** to take down major servers, highlighted the generally weak status of security in place with IoT. And we have seen little improvement since that attack and the seemingly endless stream of other attacks and breaches. In fact, **researchers are consistently finding security holes in consumer products.** For example, they recently discovered the vulnerability of a smart scale which allowed cybercriminals to steal data as it's sent from the scale to a user's smartphone app.

So what, right? Why would anyone want data on your weight and overall health? **How could that put you at risk?**

This mindset actually brings us to the root of the issue: **oversharing.** Think about all the smart devices on the market right now. From smart scales to smart cameras to smart refrigerators, if not properly secured, **cybercriminals could quite probably harvest most every single data point of our lives.** We must remember that security has just as much to do with privacy as it does with safety.

What does this mean for you? Personally, consider that **maybe not everything needs an internet connection.** Professionally, take note of our security policies and think about why they exist. You may well see that most everything we preach about cybersecurity can and should be applied to your household!

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!*

EVIL APPS AND NOT-SO-SMART DEVICES

Before downloading the latest trendy app consider this…

Last year, Google reported its removal of more than 700,000 apps that were in violation of Google Play policies, including **over 250,000 copycat apps**, which attempted to deceive users by impersonating legit versions. Google also noted that, while 700,000 seems like a big number, nearly 99% of apps with abusive or malicious content were identified and rejected before anyone could access them.

However, as with all things security, it's that one percent we need to worry about. And since it's nearly impossible for online stores to fully vet every single app that gets submitted, the onus falls on end-users to up their security awareness. ***Before downloading and installing apps on your smart devices, do some research.*** How many downloads does the app have? How many reviews does the app have and are they positive? Are you downloading from an official app store or a third-party website? And finally, consider the privacy requirements after installing. If the app asks for more access than what seems necessary, delete it and find a better option.

If you've been issued a smart device by our organization, know and follow our policies regarding what you're allowed to install and access. If you're not sure, please ask!

Convenience at a Cost

One of the most popular smart devices to hit the market, is the *smart camera meant specifically for home security*. But recently, when an owner of the Ring doorbell camera noticed odd activity on his account, he learned some unfortunate facts. Despite changing his password after he and his partner split up, it was discovered that due to a security flaw, the change in password failed to prevent his ex from gaining regular access and downloading videos. In a nutshell, the ex was able to watch his former partner, and every single visitor, come and go 24 hours a day.

Now apply these facts to things like baby and pet monitors, and suddenly, the fragile state of our privacy comes into focus. The Internet of Things does indeed provide a ton of convenience, often sacrificing security in the process.

What can you do about it? Unfortunately, the majority of solutions need to come from the manufacturers. But here's a checklist for individuals before and after purchasing new smart devices:

1. Research, research, research. Find out if the company in question has any security-related failures on their record. And read as many reviews of the product as you are able to digest.
2. Change the default username and password immediately. Out-of-the-box passwords are typically public knowledge and need to be changed ASAP.
3. Check the default settings. Only enable features that you absolutely need and familiarize yourself with permissions granted to the device and its subsequent app.
4. Update firmware/software. Devices often receive upgrades that need to be implemented ***after*** you install the device or app. Turn on auto-update where possible.
5. Occasionally double-check configurations. Sometimes firmware or software updates reset devices to default settings. It's a good idea to log into the admin side and ensure your preferred security settings are still intact.

Did you know?

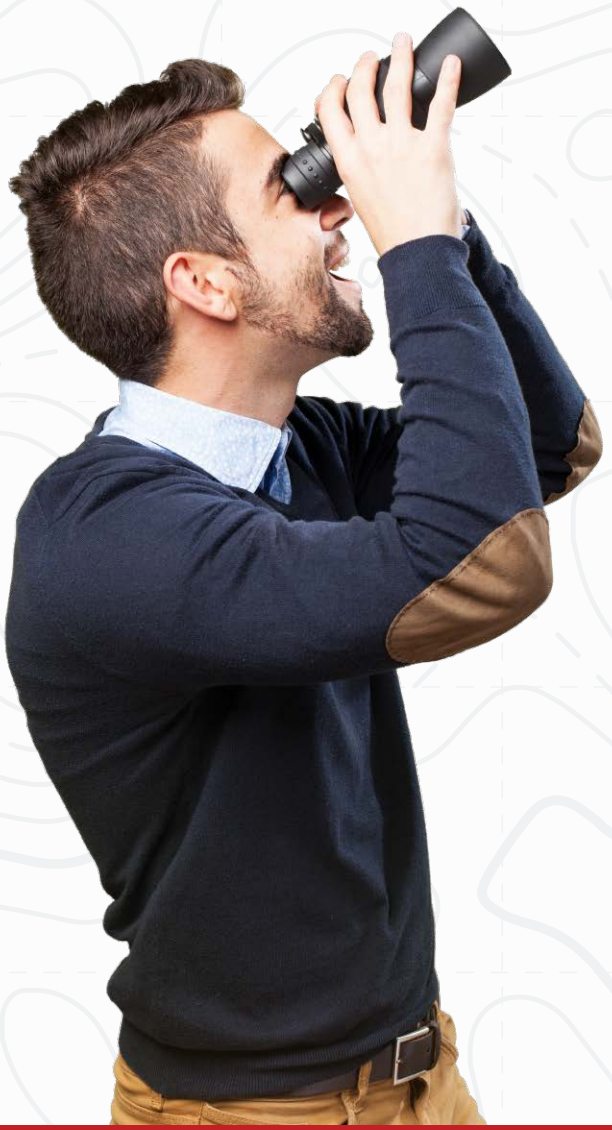
One of the simplest ways to avoid getting phished is to use the **mouse-over technique.** When you receive an email containing a link, and you're not sure of its legitimacy, simply hover over the link with your pointer and you can see the full details of the URL. You can also do this on mobile by pressing and holding (long press) the link in question and in most cases, the full URL will reveal itself.

But a word of caution: actually clicking on questionable or suspicious links is never a good idea and can easily (accidentally) happen, as you check the authenticity of that link on your mobile device. If at all possible, wait until you are on a computer and perform the classic mouse-over. You wouldn't want to unintentionally click a malicious link while attempting to long-press and view the URL for verification.

Article provided by KnowBe4

The Remote Worker's Field Guide to Security

Whether you are mobile for work or pleasure, if you need to access the internet, **remote security awareness** tacks on several additional responsibilities. Follow this field guide to help keep your devices and data out of harm's way.



Discretion is Advised.

If you're going to access sensitive information, then you should avoid sitting in the middle of a people-packed area where anyone could look over your shoulder or eavesdrop on your conversations. Seek out a more **secluded spot** with your back to the wall.

VPN or Bust!

No matter where you go, chances are you'll need or want access to the internet. Unfortunately, public WiFi, regardless if it's password-protected, comes loaded with security concerns. Protect yourself by **activating a VPN on all devices**. VPNs (virtual private networks) encrypt your connection and make it nearly impossible for a nearby cybercriminal to intercept your data.

If you like it, you'd better keep an eye on it.

Traveling alone can be challenging especially if you need to use the restroom or need to get food, as you drag bags and luggage around with you. But that's part of the gig. **Never, never, never ask a stranger to watch your things for you**, even if they work for the airport or restaurant, and even if you have access to a private lounge.

Don't get fooled by randomness.

If you happen to stumble across a random USB drive or some other form of data storage device, **do not plug it in**. Social engineers bait their victims by leaving infected drives laying around in busy areas. If you access it, your device and any networks to which you may be connected, could be immediately compromised.

Disable auto-connect.

When you join a new network, most smart devices ask if you want to remember the network and auto-reconnect the next time it's within range. Why shouldn't you allow this to happen? For one, **your device could automatically connect before you even have a chance to activate your VPN**. And there's a chance a cybercriminal has spoofed the network hoping your device will see it and be tricked into auto-connecting, effectively giving the fraudster access to the data you transmit or receive.

Always follow policy.

Whether using a device issued to you by our organization or using your own device to access data related to our organization, follow the guidelines we have in place for remote scenarios. **It's your responsibility to know and follow our policy regarding VPNs and the usage of public WiFi.** If you're not sure, just ask!

Article provided by KnowBe4

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

SECURING MOBILE DEVICES

LOCK IT UP!

Secure your device with a strong passcode, pattern, or pin, just as you would a computer.

ENABLE REMOTE ACCESS

Most manufacturers offer a service that allows you to connect to your device from your computer in order to locate it, or remotely reset it to factory default.

USE A VPN WHEN ON PUBLIC WIFI

VPNs (Virtual Private Networks) encrypt your connection and are a must-have for mobile security.

INSTALL ANTIVIRUS AND ANTI-MALWARE SOFTWARE

Never forget that mobile devices are just as likely to get infected as computers, if not more so!

KEEP IT CURRENT

The longer you go without updating, the more risk you assume. Enable auto-update to get the latest and greatest versions of software and firmware.

TURN OFF BLUETOOTH

Bluetooth is unsecure and leaves you open to snooping. When not in use, turn it off.

DISABLE AUTO-CONNECT

Cybercriminals set up rogue access points that spoof your previous WiFi connections, which allows them to seize your personal information. Eliminate this concern by disabling auto-connect.

VERIFY THE SOURCE

App stores are full of imposters and malicious applications. Double-check the source and read several reviews before installing.

THINK BEFORE YOU CLICK

Smishing, or phishing via SMS, has been around for a long time. Don't click on any links sent to you randomly by text message.

KEEP IT BACKED UP

In addition to manually backing up, there are a bunch of cloud options available at various price-points. If your device is lost or stops functioning, you'll still have your data!