BLINN.COMmunications
September 2019
179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

Portable and Dangerous to Your Data (Part Two)

Just about everybody has a mobile phone and more than 4 in 5 of us have smart phones. Those and other portable devices are convenient but dangerous, so this month we'll look at some of the steps you can take to protect your data.

For thumb drives and the memory in all portable devices, encryption is wise. But do you really need to take that thumb drive full of company files home? Many companies make it possible for employees to log in securely from home. One method uses software that establishes an encrypted connection between the employee's home computer and the computer in the office. The other option is more commonly used by people who work from home with a computer provided by the company. In that case, a secure connection is established between the computer at home and the corporate network.

People who need to take corporate data with them on a notebook or tablet, a thumb drive, or a smart phone should use encryption on the devices. This makes the data more difficult for crooks to obtain. That's not to say impossible because someone with sufficient computing resources and a strong enough need to know what's on the device will be able to break the encryption eventually. But unless you've run afoul of the National Security Agency, basic encryption will protect your data.

Those who connect via Wi-Fi hotspots, whether open or secured, should use virtual private network (VPN) software. A VPN application encrypts data when it's in the air between your device and the hotspot.

Whether your portable device uses Windows, MacOS, Android, or IOS, you'll find variety of VPN products and services for free or for a modest price. If you're protecting an Apple phone or tablet, obtain the app from the Itunes Store. For Android devices, download the app from Google Play or the Amazon App Store.

Convenient but risky: As we carry around more data on mobile devices, thieves gain new opportunities to steal it.

Today's VPN applications require little or no technical knowledge to install and use. If you know how to download and install an app, which is essentially an automatic function on smart phones and tablets, and you can create an account using your e-mail address and a password, you already know enough to set up most VPN apps. Many of the services provide the VPN without charge for limited use. If you spend a lot of time online via Wi-Fi, you will need to pay a few dollars per year for the service.

Given the amount of protection VPN provides, the small annual fee is well worth the cost.

Many VPN applications exist. I selected Private Internet Access because it supports Windows, MacOS, Linux, Android, and IOS systems. For about $3 per month, PIA protects all of my devices. Up to 10 devices can be active at any time, which would cover the active devices for even a large family.

Other Good Ideas

At the very least, password protect any device that you carry away from your home or office. Even computers that are used at home should be password protected so that private information will remain private if the computer is stolen.

Set a timeout on any portable device so that it will automatically turn off and lock when it's not in use.

Run updates frequently or allow the device to update the operating system and all apps automatically. Updates are sometimes designed to provide new features, but most updates address security flaws and you

Blinn Communications News (ISSN 2639-5762) is for clients and friends of William Blinn Communications, Worthington, Ohio. Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com.

shouldn't skip them. Windows users can delay feature updates, but should never delay security updates.

Downloading apps only from official sources such as the Apple Itunes Store, Google Play, or the Amazon App Store doesn't guarantee that they're free from malware, but it at least tips the odds in your favor.

If your mobile device has a locator option, be sure to enable it. Then if the device is stolen or simply misplaced, the service can report the device's approximate location and also might be able to engage the on-board camera to take pictures of the current user.

Use hardware encryption if the device supports it. Sometimes encryption can be used in conjunction with device-finder software to delete data from a stolen device.

Thumb drives, and any device that's used to store sensitive data, should be encrypted. Free open-source applications such as VeraCrypt can be used to encrypt standard thumb drives, but self-encrypting devices make the process easier – at a cost. A 64GB self-encrypting thumb drive sells for nearly $140 while you can buy a standard thumb drive with four times that capacity for about one fifth of the price. How much is convenience worth?

Being careful, using reasonable security practices, and adding applications that protect your privacy won't guarantee that you'll never be victimized by data poachers, but you'll make your data a much less attractive target. The harder you make a thief work, the more likely it is that the thief will forego your data and attack a softer target.

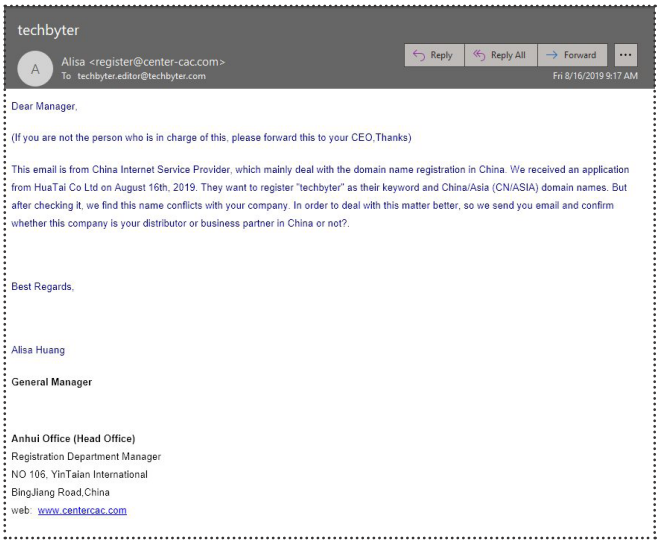
Sometimes good old-fashioned protection works, too: Have you labeled portable devices with your name and a phone number? Honest people will try to return things that they find but they can't do that if there's no way to identify the owner. Some devices place the owner's information on the boot screen. That's helpful but if it won't work if the device's battery is dead.

Security need not be complicated or expensive but it is something that needs to be examined occasionally and updated as needed. Ω

Scammers in China Want Your Money

Have you received an email that claims to be validating whether you want a company in China to be able to register your name for their website? Don't play their game.

I received an email from "Alisa <register@center-cac.com>" telling me that some company I've never heard of in China wants to register TechByter as a domain name. "Alisa" said that I should let her know "whether this company is your distributor or business partner in China or not." I deleted the message and, if you receive a similar message, that's what you should do, too.


techbyter

Alisa <register@center-cac.com>
To techbyter.editor@techbyter.com

Reply | Reply All | Forward

Fri 8/16/2019 9:17 AM

Dear Manager,

(If you are not the person who is in charge of this, please forward this to your CEO,Thanks)

This email is from China Internet Service Provider, which mainly deal with the domain name registration in China. We received an application from HuaTai Co Ltd on August 16th, 2019. They want to register "techbyter" as their keyword and China/Asia (CN/ASIA) domain names. But after checking it, we find this name conflicts with your company. In order to deal with this matter better, so we send you email and confirm whether this company is your distributor or business partner in China or not?.

Best Regards,

Alisa Huang

General Manager

Anhui Office (Head Office)
Registration Department Manager
NO 106, YinTalan International
BingJiang Road,China
web: www.centercac.com

This is not an unusual scam. It is also not a new scam. You probably won't be surprised to learn that "Alisa" really doesn't have my best interests in mind.

It's not an attempt to gain access to any of my accounts but it is an attempt to get me to pay for a wildly overpriced domain registration is China. Unfortunately, this old scam still works and so the scammers keep sending out their fake warnings.

If you respond in any way whatsoever, the scammer will try to sell you domain registrations for dozens of top level domains at inflated prices. For example:

- TechByter.asia 35 USD/per year
- TechByter.in 35 USD/per year
- TechByter.co.in 35 USD/per year
- TechByter.cn 65 USD/per year
- TechByter.com.cn 65 USD/per year
- TechByter.net.cn 65 USD/per year
- TechByter.org.cn 65 USD/per year
- TechByter.tw 65 USD/per year
- TechByter.com.tw 65 USD/per year
- TechByter.hk 65 USD/per year
- TechByter.com.hk 65 USD/per year
- Brand Name: TechByter 180 USD/per year

That would be more than $800/year with absolutely no benefit! Dealing with scams like this is easy:

Just Delete It

That's right. Do nothing other than press the Delete key. Do not respond in any way. Just delete the message and get on with your day.

You may wonder how the Chinese scammers obtained your information. Registering a domain name creates an entry in the *Whois Public Internet Directory* in accordance with the Internet Corporation for Assigned Names and Numbers (ICANN) as part of the domain name registration process. Anyone can view this directory.

If you do business in China, you'll probably want to register names with a "cn" top-level domain but you don't want to do that with scammers. Your company's international business division will take care of it.

So it really is just this easy easy: Ignore the message and delete it. Ω