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

Keys to Keeping Crooks' Eyes Away from Your Data

How safe is the phone, thumb drive, or computer you carry around? Having a device lost or stolen is more than just inconvenient. Beyond the inconvenience and cost to replace the device, there's the consequences of lost data.

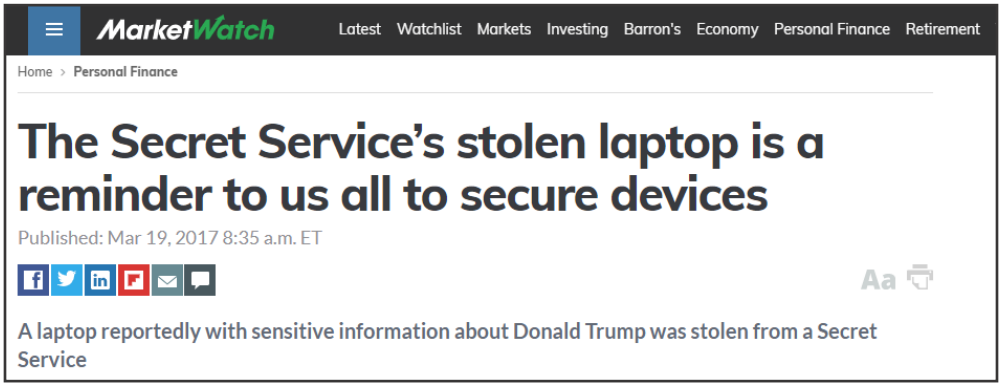
Maybe you think your portable devices are safe and that you'd never lose one or allow it to be stolen. I know someone who left a notebook computer unattended for a few moments at a conference and returned to find that it had been stolen. He was in the same room with the computer, but was briefly distracted. That's all it takes.

In fact, agents from the Federal Bureau of Investigation lost or had stolen 160 notebook computers in a four-year period. At least ten of them contained sensitive information. Earlier, the bureau had more than 300 laptop computers stolen in a little over two years. Those who work for the FBI are trained to be careful and yet they routinely have electronic devices go missing.

Even the Secret Service has had computers stolen, including a 2017 event in which a notebook computer was stolen from an agent's vehicle in New York City.

Portable devices such as thumb drives, smart phones, notebook computers, and tablets are among our most powerful tools, but they can also be gigantic security holes that allow access to your personal data and your company's proprietary data.

A group of hackers released one million device IDs for Apple phones in 2012 after they stole an FBI laptop computer that gave them access to the agent's desktop computer where the device IDs were stored. The file contained data that uniquely identified the phones and included user names, device names, device types, postal codes, smart phone numbers, addresses, and more.


MarketWatch Latest Watchlist Markets Investing Barron's Economy Personal Finance Retirement

Home › Personal Finance

The Secret Service's stolen laptop is a reminder to us all to secure devices

Published: Mar 19, 2017 8:35 a.m. ET

A laptop reportedly with sensitive information about Donald Trump was stolen from a Secret Service

If you consider your portable electronic devices to be safe from theft, understand that even Secret Service agents can have computers stolen from their cars.

If something like this can happen to multiple FBI agents every year, it can certainly happen to you. Theft of a physical device is only one threat to be aware of, though.

Convenience or Security?

We want convenience and we want security, but these desires can compete with each other because security measures often make devices more cumbersome to use and making a device easy to use may reduce its security.

The cost of security, both what you'll pay for software, hardware, and services, as well as costs that result from reduced ease of use, must be balanced against the potential cost of lost data.

Thumb drives that can hold 512GB of data cost less than $100 and 64GB drives are available for about $10, so the amount of important information that can be carried on a device that's easy to lose is nearly incomprehensible. A standard page of information would consist of about 2000 characters, so even a "small" 64GB drive might contain more than 33 million pages of information.

If you carry important information on a thumb drive or on a computer, the device should be encrypted. Some thumb drives include encryption software and applications such as the free VeraCrypt (veracrypt.fr) are available for download and installation with either a thumb drive or a mobile computer.

Organizations that deal with personal identification information and data covered by the Gramm-Leach-Bliley Act of 1999 generally encrypt that information when it is being passed through the network and when it's stored on servers or employees' desktop computers. The most careful organizations encrypt both the connection and the files that are being transferred.

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.

Thumb drives are less common now that files can easily be stored on Google Drive, One Drive, and various other on-line services. That eliminates one type of security but adds another type of threat.

Cloud-based storage systems usually encrypt the files on their servers and establish encrypted connections when users are uploading or downloading their files. The only exceptions would be for those who set up their own file transfer protocol (FTP) site and who transfer unencrypted files over a non-secure connection. If you're using a commercial service, your files are stored safely.

But what if you hand someone your user name and password? It's not something you'd do intentionally, but its easy to do accidentally.

Using Wi-Fi hot spots in restaurants, airports, and even libraries can be dangerous unless you install and use a virtual private network (VPN) application. Nearby users can view clear-text connections with Wi-Fi devices and it's not difficult for someone in a busy airport or coffee shop to connect to the location's legitimate Wi-Fi system and then create a spoofed hotspot that attracts other users. This makes it possible for the person running the scam to collect any URL, user name, and password you type if you're not using a VPN.

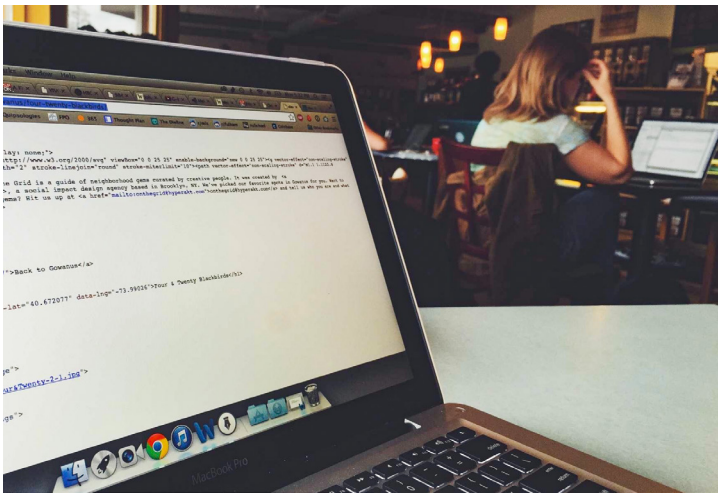
Phones and tablets are a double threat because they usually come with large amounts of built-in memory and they can communicate wirelessly over non-secure networks. Thieves have two opportunities: They can steal the physical device or they can intercept data as it's being transmitted to an open Wi-Fi hotspot.

Are You Scared Yet?

Regardless of what security measures you have in place, it's a good idea to avoid the use of banking applications and such via public Wi-Fi. Good protection against basic threats isn't particularly difficult, though.

Never leaving a phone, tablet, or computer unattended, even for a few seconds, is the best way to avoid losing the physical device. For thumb drives and the memory in other portable devices, encryption is a good idea. Encryption doesn't guarantee the safety of your data, but it skews the odds strongly in your favor.

Protecting data and log-in credentials during transmission from your device to a Wi-Fi hotspot requires only the installation of VPN software. Some services are free and even the ones that charge aren't expensive. A VPN does slow the connection in most cases, but not objectionably.



Someone sitting nearby in a restaurant, airport, or coffee shop can create what looks like a legitimate Wi-Fi hotspot.

Regardless of the type of portable device you use, you'll find variety of VPN products and services that are available from Apple's store, Microsoft's store, and Google's store. Relying on *official* channels for apps won't absolutely guarantee that you'll never download malware, but it does provide some assurance that the app you've selected has been validated.

VPN applications require little technical knowledge. Anyone who knows how to download and install an app and who can log in to an email account already knows enough to set up most VPN apps.

Consider the Basics

Remember when your mother used to sew name labels into your clothes? No? Well, once upon a time, doing that was commonplace. It was a good way to retrieve a misplaced hat or glove.

- Label portable devices with your name and a phone number. You might be surprised how many people actually attempt to return things that they find, but they can't do that if there's no way to identify the owner. Many phones and tablets have a screen that can identify the owner, but if the device's battery is dead, it won't work. A label is a good idea.
- Password protect the device. That should be evident, but a surprising number of people carry around devices that aren't password protected and also aren't encrypted.
- Set a timeout on the 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 shouldn't skip them.
- Download apps only from official sources such as the Apple Itunes Store, Google Play, or the Amazon App Store. Malware has been distributed via these channels, but the likelihood is reduced. Apple's process is considered to be the strongest of the bunch.
- Services exist that will attempt to find your mobile device if it's lost or stolen. 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. Various services exist and some are specific to certain types of devices.
- 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.

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.

Security experts know that basic protection for a home or business that makes a thief work harder can convince the thief to forego your house or business. The same is true for data because the thief will seek out a softer target to attack. Ω