nLightenedThoughts

February 2014

William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

Yes, Someone Really Can Steal Your Data

IF SOMEBODY HAS SUFFICIENT RESOURCES AND WANTS YOUR DATA, THEY WILL GET IT. TOTAL SECURITY IS IMPOSSIBLE AND I'VE HEARD PEOPLE USE THAT AS A JUSTIFICATION FOR DISREGARDING SECURITY ALTOGETHER. GIVING UP IS NOT A GOOD RESPONSE.

It depends on how much time and patience crooks have and how much computer power they can bring to bear.

Security exists on a continuum and passwords, your first line of defense, may not be as strong as you think they are. If you think that you have created secure passwords, but your accounts are routinely hacked, then you haven't created secure passwords.

Common sense would suggest that passwords such as these will be on a crook's first-guess list: password, password1, letmein, abc123, and 123456. Even so, these are all commonly used.

Password Safety Tips

- Never write a password down.
- Don't re-use passwords on sites that contain financial data.
- Use complex passwords that are at least 8 characters long.
- Use a password manager.

Password management systems such as LastPass store all of your credentials locally and on the LastPass server so that they are readily available to you. The password files are encrypted both on the server and on your computer. You need to create a strong, secure password for access to the password manager, but that becomes the only password you need.

The password for the password manager needs to be sufficiently complex that it will be difficult to break and yet easy to remember. It is possible to create a strong password and then, even though you shouldn't write the password down, you can write clues that will be meaningless to anybody but you.

Let's say that you lived on Chesterfield Drive in 1967 and that you toured Draveczky Castle in Romania during a vacation in 2005. Here's how you might use that information to create this password: **Chesterfield#1066Draveczky**. That's a 26-character password and you could write a plain-text reminder like this:

1967 hash Norman castle

- **1967** is your memory cue for Chesterfield.
- **Hash** is your memory cue for the pound sign, hash sign, octothorpe, or tic-tac-toe—whichever term you prefer.
- **Norman** is your memory cue for 1066, the year that the Normans invaded England.
- **Castle** is your memory cue for Draveczky

By themselves, the words would be meaningless to anyone who happened to find them.

I have used "NYPL" as shorthand for **42NDSt@5thAve** (the New York Public Library's main branch is located on 42nd Street at 5th Avenue) and "Tischman and City" for

Total Security for Your Computer (Almost) Guaranteed

Several years ago, as part of a radio interview, I described how it might be possible to make a computer completely secure. Start with a computer that has no input or output devices except for the keyboard, screen, and mouse. No printer. No phone line in the room. No network.

Place the computer in a room that's located in the center of a building. The walls, ceiling, and floor should be reinforced with ¼-inch solid steel plates.

The room would have no windows and only a single door, which would be observed at all times by at least two armed guards. The building would be protected by a Faraday cage.

The person who uses the computer may not take anything into the room or bring anything out. The armed guards are able to observe the computer user at all times by means of closed-circuit television cameras; the cameras are positioned so that the guards cannot view what it on the computer screen.

The computer is connected to a power inverter that is itself powered by a 12-Volt battery that the user brings into the room.

This computer would be highly secure, but essentially useless.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085.
Phone 614.859.9359. On the Web at www.n-Lighten.us. All rights reserved.

666FifthAve&NYC (the Tischman Building is a 666 Fifth Avenue). Needless to say, I won't be using those again for anything.

Securing Portable Devices

A poll in 2011 by Confident Technologies shocked me by reporting that more than half of the people who use portable devices (smart phones, notebook computers, and tablets) don't bother to protect them with a password or PIN. Lose an unprotected device and you have just given away any data that's on it.

Even the FBI occasionally loses portable devices or has them stolen.

Some users of portable devices and Apple computers seem to think that they are safe from malware and viruses. I talked with a security expert for McAfee late last year and he confirmed that millions of viruses are targeted at Windows machines, but thousands of malware applications target Macs and tens of thousands target portable devices. The threat may be smaller, but that doesn't mean it's non-existent.

Using portable devices in public can be dangerous. Restaurants, libraries, and some municipalities offer open Wi-Fi access. These connections are safe for Web browsing, but they can be dangerous if you use them to connect to an office or home computer that contains data you want to keep private.

Software is available to create a virtual private network that encrypts your data when it's in the air—SurfEasy, for example. If you use your phone, tablet, or notebook computer with Wi-Fi hotspots, you need to enable a VPN.

The Bottom Line

Technicians sometimes refer to "PEBKAC" errors, "problem exists between keyboard and chair." In other words, the user has created his or her own problem. We all like to blame the application or the operating system, but in most cases it's us, the humans, who cause the problems.

Regardless of what antivirus or antimalware applications you have installed, security must be managed between the keyboard and the chair. If you find something that seems too good to be true, remember what you mother told you: *It probably is too good to be true.*

Security may never be perfect, but with a little caution and a bit of planning you'll be able to create an environment that's sufficiently secure that you'll convince the crooks to look elsewhere for easier targets. Ω

Will the FCC Appeal the Net Neutrality Decision?

And should you care? Yes, you should. And I certainly hope so. There are dire predictions about what cable companies might do. Will they?

There's a difference between what's possible legally or technically and what works as a business model, but it's still worrisome.

The appeals court struck down the Net neutrality rules on a technicality, but affirmed the FCC's poisition as the regulator of broadband services.

The court said that the FCC improperly classified service providers, so the FCC could fix the problem by properly classifying cable operators. It's more likely to appeal the decision to the Supreme Court.

Net neutrality gives everyone equal access to the network: Your site or mine should load just as quickly as one from the New York Times or Amazon. Intentional slowing of data because of its source would be disallowed.

Somehow this has become a political argument instead of a techical discussion. It began in 2007 when users accused Comcast of blocking peer-to-peer services such as BitTorrent to manage its network traffic. A year later, the FCC released a decision against Comcast.

Politics has no place here. Congress could pass legislation to set the rules, but given the gridlock in Washington, that's about as likely as a moon landing by the Taliban.

We are faced with the possibility of having two separate and unequal Internets, one for organizations with enough money to pay for faster service and another for everybody else. This would automatically favor large, rich corporations and stifle start-ups that couldn't pay enough to buy the bandwidth that would allow their sites to perform well.

The Wrong Direction

At a time when many countries are doing everything they can to provide high-speed Internet access to all citizens and at reasonable prices, the recent court decision poises the United States to embark on a path in the opposite direction.

The wealtiest people would enjoy exellent service and the rest of us have slow service that's not usable for more than e-mail.

I doubt that the worst will happen because the owneres of cable systems are probably smart enough to know that if they render streaming music and streaming video unsuable, customers will abandon the service. Their business model and that of for Netflix and Amazon won't work if their only customers are member of the one percent.

Today, the Internet is a utility like water, gas, or electricity. The rich may use more of these utilities, but access to the services is the same regardless of where you live or how much you have in the bank. That's the model the Internet should follow.

Gas, water, and electricity are all regulated. The Internet should also be regulated. Ω

n-Lighten.us
Division of William Blinn Communications

179 Caren Ave., Worthington, Ohio 43085
614/859.9359 • www.n-lighten.us