SIM2K
Adapting Technology to Your Business Needs

5•16
Information you can use

SIMformation

5 Tips for Safe Computing

You mean to practice safe computing habits, really you do. But when you fire up your computer, you just want to get stuff done – and that's when even savvy users begin to cut security corners.

We'd all do well to take a lesson from truly paranoid PC users, who don't let impatience or laziness stand in the way of protecting their data. Here are some "reaaalllyy secure" tips you might want to incorporate in your use of IT:

1. Use a VPN
A perennial concern of the security conscious is having an interloper listen in on online activities, which can make you a ripe target for phishing attacks or even result in a hijacked connection. This could happen in a variety of settings, including at unprotected public Wi-Fi hotspots or hotel access points compromised by those targeting business travelers.

It makes much more sense to access the Internet through a virtual private network (VPN) in which all outgoing and incoming traffic is funneled through an encrypted channel to a trusted Internet gateway. You can obtain a VPN from some commercial offerings for about $5 to $10 per month. However, this is a technical task that would be better left for SIM2K to set up for you. This also will reduce the chance that a "pay to use VPN" service will not suddenly go "dark" on you and leave you hanging for this service. so please contact us if you would wish to have a VPN connection established for you.

2. Enable two-step or two-factor authentication for your online accounts
Basic password protocol of creating lengthy, complicated passwords/passphrases, using different passwords/passphrases for different accounts and managing them all with a password manager, is still an important security fundamental, but it isn't nearly enough to protect your computer in 2016.
Having a second, dynamic code that is generated on the fly and delivered via an alternate, trusted route overcomes some of the inherent vulnerabilities of a static password and increases the likelihood that your account will stay safe even if your password is compromised. The most common form for this security measure is to have a one-time code sent by text to your cell phone to use when logging into an account. Even more secure are two-factor authentication methods where codes are generated on a device itself, such as mobile phone apps that are primed to generate one-time codes on demand, hardware security fobs or multi-factor authentication devices like fingerprint readers.

3. Always lock your PC
One habit that most users are aware of but few practice is to ensure that laptops or desktop PCs aren't left unattended and unlocked, even in a semi-private space like the company office. Given that many users log in to their computers as administrators, it takes just a few seconds of unfettered access to a running PC to install some form of malware or spyware tailored to evade detection by popular antimalware software. The solution is to password-lock your device if you will be away from it, protecting your data while leaving running apps and the desktop untouched. On a Windows PC, press the Windows key + L. Upon your return, you'll need to type in a password to unlock the device, but this minor inconvenience is worth the added protection. Even if you are in the habit of manually locking your computer, it's still a good idea to set it to automatically lock after a period of inactivity as a hedge against the one time you forget to manually lock it. SIM2K can set a network policy to automatically lock users' PCs if inactive for some time.

4. Encrypt your drive
Encrypting the data on your PC is an important step in ensuring that your data isn't compromised. Encrypting the drive means the data on it will show up as gibberish if your laptop is stolen and the thief tries to access the data or if the hard drive is ever removed and loaded on another system. Windows 10 can encrypt your drive by default, but again, this is a complex situation that is best left for SIM2K to set up for you, as encryption done wrong means that your data might not be recoverable, so let us assist you with any drive encryption.

5. Make sure your own Wi-Fi network is secure
Home and small-business Wi-Fi routers and access points (APs) are something we tend to set and forget, but it's worth spending half an hour performing a security audit on your network and shoring up any weak points. Because wireless signals can reach outside your walls, it's critical that you defend against eavesdropping and connection hijacking. For simplicity's sake, most small-office and home networks use a static password or passphrase as the encryption key to protect transmitted data, which could be hacked. While complexity (using mixed case and special characters) matters, having a longer length of at least 20 characters (even longer is better) will probably have the greatest impact on making it harder for the bad guys to crack. It is also wise to keep your internal business traffic on one network and set up a second wi-fi network for visitors that does not allow access to internal devices, for sake of security.

Phishing Attack Firing

Punishing the victim of a crime feels wrong, but that's exactly what happened to one unnamed employee at Alpha Payroll Services in Trevose, Pennsylvania. The firm recently disclosed they were the victim of a Phishing scam targeting W-2 data that was compiled for their customers.

In a letter dated April 29, published this week by the New Hampshire Attorney General's breach notification website, an attorney for Alpha Payroll disclosed that the company compromised client W-2 records after an employee fell victim to a Phishing scam. In early March (March 1st or 2nd), the letter states, someone impersonated Alpha Payroll's CEO and requested "copies of all the 2015 W-2 forms produced by Alpha Payroll on behalf of its customers."

Clearly, the email was believed to be legitimate, because the employee who received it complied. Later, on April 8 – after an Alpha Payroll customer reported their staff had fraudulent tax returns filed under their Social Security Numbers – an internal investigation discovered the successful Phishing attack.

"Alpha Payroll leadership promptly terminated the employee, hired experts to assist in the investigation and response, and has been in contact with law enforcement, including the Criminal Investigation Division of the IRS and the FBI, regarding the incident," the letter explains.

The employee, victimized by the same person who later victimized Alpha Payroll clients, was fired because they believed the email was legitimate. "If you fire every employee who clicks a Phish you will soon have no employees," commented one security expert. "While anti-Phishing training may reduce the number of incidents, it will never be 100% effective. It only takes one person to click, even by mistake. You need to assume that a Phish will succeed, that bad guys will get in. It's what you do after the attack that matters."

In addition to terminating the victimized employee, Alpha Payroll says they are redoubling their efforts to "educate employees on phishing schemes and the importance of confirming the legitimacy of e-mails to lessen the likelihood of future incidents."

However, many HR experts believe that this firing sends the wrong message to employees. "The purpose of security awareness training is to educate employees and teach them how to avoid the same mistakes in a real situation. Firing them won't help anyone and would probably end up costing the company more in having to find and train a replacement," said a security expert that provides training in this area. "Not to mention, how can you fire someone if they didn't know they were doing anything wrong?" he asked.

SIM2K has a variety of programs in place designed to help minimize the impact of Phishing attacks and to help you train your employees to avoid this very sort of incident or even more serious events such as unleashing a ransomware program on your network. Call us for details on how we can help you protect your network.

Internet Sales Taxes

A new South Dakota law may end up determining whether most U.S. residents are required to pay sales taxes on their Internet purchases.

The South Dakota law, passed by its Legislature in March, requires many out-of-state online and catalog retailers to collect the state's sales tax from customers. The law is shaping up to be a legal test case challenging a 25-year-old US Supreme Court edict that prohibits states from levying sales taxes on remote purchases.

Unless courts overturn the South Dakota law, it will embolden other states to pass similar Internet sales tax rules, critics said. The law could "set the course for enormous tax and administrative burdens on businesses across the country," said the e-commerce trade group NetChoice. If dozens of states adopt Internet sales taxes, online sellers could face audits and changing tax rules in thousands of taxing jurisdictions nationwide. Even with software that could make tax calculations easier, that would be a burden, NetChoice says. And online shoppers could end up paying up to 10% more for many products.

Supporters defended the law. "It's time to provide a 'level playing field' for bricks-and-mortar retailers that are required to collect sales taxes," said a South Dakota state senator. With South Dakota's sales tax going up from 4% to 4.5% in June, out-of-state sellers have an advantage.

Even before the law went into effect May 1, it prompted two lawsuits. The state sued four online sellers, including Newegg and Overstock.com, in an effort to force them to register with the state and collect its sales tax. The law requires out-of-state retailers to collect sales tax if they have more than US$100,000 in sales, or 200 remote transactions, in South Dakota each year.

Then, on Friday, NetChoice and the American Catalog Mailers Association sued the state, arguing the new law violates the 1992 Supreme Court's Quill v. North Dakota decision. South Dakota lawmakers passed the law "with the express understanding that its terms contradict" the Supreme Court, lawyers for the two trade groups wrote in their lawsuit. The law is "plainly unconstitutional" because it usurps the U.S. Congress's authority to regulate interstate commerce, they said.

In the Quill decision, the Supreme Court ruled that states could not impose sales taxes on sales by out-of-state retailers because the taxes, with varying rules across thousands of jurisdictions, would be burdensome for sellers to collect. After the ruling, retailers with no store or warehouse in a state were not required to collect the state's sales tax.

The court left an opening for the U.S. Congress to streamline sales tax collection and allow states to extend it to out-of-state businesses. Lawmakers in Congress have been trying to pass Internet sales tax legislation for more than a decade, but opponents have stalled it.

FBI Addresses Ransomware

With the rise of more extreme Ransomware attacxks, the FBI is weighing in and asking companies (and individuals) to be more vigilant in examining practices to guard against infections. Here are the tips that the FBI is recommending:

Tips for Dealing with the Ransomware Threat

While the below tips are primarily aimed at organizations and their employees, some are also applicable to individual users.
Prevention Efforts

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure anti-virus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

Business Continuity Efforts

- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

SIM2K has been recommending that companies take these precautions, and has developed programs that you can use to help protect your network and data from suffering any major impact from a ransomware attack.

No control is 100% effective, but by maintaining several layers of control, businesses can mitigate the ransomware risk. Should you run afoul of an infection, call us immediately as there are steps that can be taken right away that will minimize the spread of the encryption and protect your files from being compromised. Please call us for more information on how to be prepared to defend against these attacks.

"Random Tid-Bytes"

Google Slides target dull PowerPoint Presentations

Google Slides aims to eliminate PowerPoint. At least, Google hopes it can, particularly among educators. Three new features aim to make presentations more of a two-way experience. They're available now on Android, iOS and the Web app. Audience members can ask questions and vote for which questions should get answered. Plus there's a virtual laser-pointer (but do not stare into it with your other eye). Q&A and voting will give your audience something useful to do with their phones, rather than searching for ways to hurt boring presenters.

E-Mail Treasure Trove - For the Bad Guys

Tens of millions of stolen credentials for Gmail, Microsoft and Yahoo email accounts are being shared online by a young Russian hacker known as "the Collector" as part of a supposed larger trove of 1.17 billion records. A security company says it has looked at more than 272 million unique credentials so far, including 42.5 million "new" user ID/passwords. The company discovered the breach when its researchers came across the hacker bragging in an online forum. Some 40 million of the credentials came from Yahoo Mail, 33 million were from Microsoft Hotmail, roughly 24 million were from Gmail, and nearly 57 million were from Mail.ru (a Russian e-mail provider). Thousands of others came from employees of large US companies in banking, manufacturing and retail. Therefore, if you have an account with one of these e-mail services, you may want to consider changing your password or establishing the password recovery features companies like Google and Yahoo offer so you are not locked out of your account should it be compromised.

What a Mickey Mouse Printer this is ...

Disney Research has filed a patent for a 3D printer that uses high-intensity light to harden a photo-sensitive resin in a single process, removing the need for time-consuming, layer-by-layer printing. The patent describes a machine for printing in "a nearly instantaneous manner." Unlike single-layer printers, Disney's proposed printer would not harden resin by drawing the outline of an object layer-by-layer. Instead, the entire object would be projected into the center of the resin, creating a whole model at once. The patent describes a using various wavelengths of light (in the blue, violet and ultraviolet spectrums). The 3D printer would use resins that cure with these invisible wavelengths that are less affected by ambient light. The photosensitive resin would also need to both absorb and transmit light at the curing wavelength. The printed object, which would be supported by the thick resin itself, could simply be lifted out once it was finished. No word if the printer says "Bippity-boppity-boo" as it produces the item.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 754th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Windows 10 Migration Path

Windows 10 is reaching the point in the operating system's maturity that SIM2K is no longer asking clients to avoid including this OS into their business network. There have been several major updates to Windows 10 since its introduction, and so we believe that we have reached a point of stability. Also, most software on the market today has been updated to run on Windows 10, so there are less chances that upgrading to Windows 10 would find software not working in this new environment. However, it is still wise to test Windows 10 in your environment before buying.

This is not to say we are encouraging any company to rush out and upgrade Windows 7 machines to Windows 10, but rather, if you are now purchasing new hardware with Windows 10 pre-installed, it is OK to run that operating system and not take the time to roll back. Windows 7 continues to be a very stable platform and will be supported by Microsoft until at least 2020, so there is no need to incur the expenses of upgrading existing Windows 7 machines - continue to use them "as is" for some time.

We also advise that you slowly integrate Windows 10 into your environment. This is especially true if you are running older versions of software, or have some legacy software programs still running. If you are a generation or two behind on your updates (for example, running QuickBooks 2009 instead of 2016) you may find some features are not compatible with Windows 10. Therefore, we recommend testing all software on the network before putting a Windows 10 machine into full use. SIM2K will be glad to help you test Windows 10 on your network – just call us before you buy.

However, it you are interested in upgrading to Windows 10, the path will be less stressful this time around than the leap from Microsoft XP to Windows 7. Enterprises should have an easier time migrating from Windows 7 to Windows 10 than they did the last go-round when they left behind Windows XP, an analyst said, citing lessons both Microsoft and corporations learned. "Microsoft has provided the option to roll out Windows 10 using most of the same processes you used with Windows 7," said a Gartner spokesman. "For that, you get a new OS, but you don't get new capabilities. Later, you can make the decision to, say, turn on the tighter security of Windows 10, or change the way that applications are distributed."

The migrate-but-then-do-more-later plan should make the transition smoother and faster than the one businesses struggled to complete in late 2013 and early 2014 as they purged XP.

The migration-to-10 process will likely take significantly less time than the upgrade to Windows 7, but not only because enterprises can reuse most of the same tools and policies. Other factors that point to an easier-this-time OS bump, said Gartner, include improved application compatibility because many organizations went through the work of recrafting internal apps or stepping up to more modern software, or services that replaced software, during the move from XP to Windows 7.

In a report Gartner released, the company contends that the upfront prep time for 10 should amount to between nine and 12 months as enterprises gather information, create and test images for deployment, then test and pilot the results both in lab-like settings as well as with small groups of users. By comparison, companies spent twice that preparing to move to Windows 7.

But while managing a Windows 10 upgrade should be easier than the XP-to-7 shift, there are considerations for adding this new operating system. Windows 10 will be updated more frequently, so companies will have to take this into account in their planning. This issue here may be that these updated from Microsoft might "break" a system, as we have seen in the past when an update disables some function or causes unexpected problems with other software programs on the network.

Gartner still expects most enterprises to spend 2016 prepping for their Windows 10 migrations, with the work beginning next year and hitting its peak in 2018.

Currently, Windows 10 is on pace to power 20% of all Windows desktop systems by the end of June, or around the time Microsoft issues its next major upgrade, according to data published in early May. Analytics vendor Net Applications pegged Windows 10's user share – a proxy for the percentage of personal computers worldwide that ran the OS – at 15.3% in April, a 1.2% point increase from the month prior. Net Applications tallied unique visitors to clients' websites to come up with its measurements.
The new operating system's growth last month was smaller than in January and March of this year, but larger than February's.

Windows 10 accounted for about 17.3% of all Windows; the difference between its user share of all PCs and only those running a version of Windows stemmed from the fact that Windows ran 89% of all personal computers, not 100%. Using Net Applications' data for the last 12 months, it is calculated that Windows 10's growth line should crack the 20% mark by the end of June, when it will power just over 300 million machines.

If you have any questions about Windows 10 and adding new hardware on your network, please call SIM2K.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com