SIM2K
Adapting Technology to Your Business Needs

10•18
Information you can use

SIMformation

Smartphone Addiction

This discussion appeared in Computerworld and presents some food for thought about the direction of technology and its impact on all users.

People all over the country, and in fact all over the entire world, have become addicted to their wireless smartphone, apps and services. And it's only getting worse with every year that passes. New apps that help us manage, monitor, use and do everything in our lives are popping up every day. We love what this technology can do for us. We talk about it, but we don't discuss how addictive these are to us.

We've all watched in amazement as the wireless industry has grown and changed, time and time again over the last several decades. During the last decade the industry has become a very different place. Growth has exploded with the Apple iPhone, Google Android and Samsung Galaxy smartphones. Apps have exploded from a few hundred a decade ago, to more than two million today.

Expect this wireless explosion to continue its rapid growth wave. More carriers are offering smartphones. More companies are offering other technologies like pay TV in competition with the cable TV industry. That's why cable TV is moving into the smartphone world. Today, cars are starting to be equipped with new wireless and interactive technology. We get updates to our automobile navigation and dashboard applications, wirelessly. In fact, every industry is jumping onto this same bandwagon.

Artificial intelligence is also starting to move into this same kind of addictive space. When we use our Google Home or Amazon Echo for everything, it creeps deeper and deeper into our souls. While this technology is amazing and we all love it, we must realize every step we take forward into this addictive land will have an impact on our lives going forward.

Now these AI services like Apple Siri, Google Android, Microsoft Cortana and more are moving into our cars, our refrigerators, everything. As this continues, the risk gets higher and higher that we will lose our ability to take care of ourselves without it.

Wireless is the center of the universe. That's the good part if you are a wireless company, worker, investor or customer. However, as users, we also must pay attention to the addictive slice of the pie.

In fact, addiction goes beyond the smartphone. We live in an addictive world. Companies think of ways to build an addictive product line. The benefits are obvious. When your customers are addicted, they come back time and time again, just like a drug addict or alcoholic.

Legal addictions are a great business model. They lead to continued growth. However, this can be a problem for those who are addicted. Consider the cigarette industry and how that has been impacted over time. Cigarettes are legal, but they are also harmful to your health. Cigarettes were around forever, and no one ever knew they were a problem. Decades later we learned over time. Could the same thing happen with our addiction to technology?

Going forward will we find that technology addiction will ultimately be harmful to our health? If so, will the government step in with their massive efforts to educate and impact growth? We are just starting to open this door with complaints of privacy invasion and all sorts of other problems.

Finally, we are starting to talk about this kind of problem. Finally, pressure is starting to be brought to bear on companies who have used this to grow, without concern for the mental health of their customers. This wave will continue to build.

Social networks are another addiction. Regular users of Facebook, LinkedIn, Twitter, Instagram and others can understand their addictive nature. So are digital games. There are often news stories about addicted players who check out of life, stay in their pajamas all weekend and play these games without eating or sleeping.

Addictive businesses are what many try to create. It's a natural for business growth and success. While this has never been a problem in the past, suddenly we are paying closer attention to this growing addiction problem. Believe it or not, that's a good thing. Every one of us needs balance in our lives. We can have a good mix of strong growth while watching out for the addiction problem.

This is not to say you can't love what we do on a daily basis. But when we cross over the line and become addicted, it can take its toll on the rest of our lives. Just ask those who are dealing with drug or alcohol addiction. So many of us have seen the damage this can do to people we know and love.

New technology like smartphones and wireless service is transforming our lives. However, for our own good, going forward we must take special care with the way we handle these topics. It's better if the companies understand these problems and solve them on their own. When the government steps in, it's often overkill.

So, we are just starting to understand the problem. That's step one. The next step as we keep learning more is, what will each company and each industry do to deal with this threat. Growth should continue, but we must be responsible and make sure we care for ourselves in the process.

The path we take going forward is up to the companies and the industries. It will be interesting to watch this issue develop over time and see the different ways companies react.

Data Breach Costs Rise

Uber announced a $148 million payout for a 2016 data breach that went unreported for more than a year as the company tried to "hush" details. These payouts are not uncommon. The average cost of a data breach has risen to $3.86 million, according to IBM's annual study. It shows a 6.6% increase in costs, including direct losses, indirect costs related to time and effort dealing with the breach, and lost opportunities such as customer churn as a result of bad publicity.

The study showed that the size of an average data breach is now 24,615 records, a 2.2% increase over 2017. Each record lost costs abut $233 in the US. The final cost is impacted by how prepared the company is to react to a breach.

US companies face the highest costs with an average of $7.91 million per breach. Globally, 23% of organizations are likely to suffer at least one breach in the next 2 years. Companies in the health and financial sectors face the highest costs per record, up to $400 each. Financial services are the most frequent victims, followed by the manufacturing and technology sectors. The level of regulation plays a large role in what a company will pay to recover from a data breach.

The IBM study found it now takes 197 days to identify a breach and 69 days to contain it. Entertainment and healthcare organizations take the longest time to discover a breach (averaging more than 300 days) while financial services and energy are quickest at discovery and remediation. Taking more than 100 days to discover a breach can add as much as $1 million to costs, as will taking more than 30 days to contain the breach, showing the importance of having detection tools in play and a remediation plan in place. In the US, data breach notification costs top out at $740,000 per breach due to notification regulations, however the new European GDPR law will rival US costs now for companies suffering a data breach.

IT experts say that using encryption, automating security and having a response team can all help reduce the cost of breach, as can employee training and cyber-insurance. Companies must have a plan in place and everyone in the company must know their role in advance, and also must identify those external partners to involve in the event of a breach.

Companies that are prepared for breaches are more likely to keep costs down due to the fact they are ready and act quickly in the wake of an incident. This includes having legal teams that understand the ramifications of a breach, communication teams preparing the messaging and the company leaders ready to take responsiblity. Customers demand the highest profile person in the company communicating what happened, what's being done and what assurances the company can give. For many SIM2K clients, this may all fall on one person, so it is important to plan ahead and know what steps to take should there be a data breach. SIM2K can assist with employee training, testing defenses and preparing responses to a breach. Call us for more information.

Passphrases Better?

The National Institute of Standards and Technology (NIST) has issued a recommendation that flies in the face of current password security – don't use "complex" passwords. NIST notes that times change. Hacking methods change. What used to stop the day's most popular attacks no longer works quite as well. It should be expected that attackers moved on to other, more successful methods once passwords started to get harder to crack.

Passphrases (or PassSentences) are, as the name infers, a full-thought-out string like "I like to go to the beach to get a tan." Experts believe that a 25-character minimum will be harder to crack. Others doubt this, as they believe that while using 25-character or longer passwords might make password cracking harder to pull off, it increases the risk that users will reuse the same password across different security domains, which is what NIST's latest advice is trying to prevent. NIST sees password reuse as one of the biggest, if not the biggest, risk to using passwords.

Implicit in the recommendation of using longer passwords (or passphrases) is the idea that increasing length provides protection. It does – in theory – but just as password complexity fails between theory and practice, so, too, does the protective capabilities of length. Most "complex" English passwords begin with an uppercase consonant, followed by a lowercase vowel, and if a number is required, it's a 1 or a 2 placed at the end. If special characters are used, they're likely to be a ! or @ or # or $. Some derivation of that password will be used across multiple security domains and only be slightly different between forced password changes on the same site (e.g., Tadpole1, Tadpole2).

Unless your password is truly random—meaning in most cases that a random character-picking program creates your password – the chosen complexity really doesn't add much cracking difficulty to the password. If you do have to use a truly random password, who wants to enter in a password like Qz&y1$Bh all the time? The problem is that most humans, if allowed to pick their passphrases, will use many of the same words and a common sentence structure, thereby negating much of the advantages of going to a longer passphrase.

The lack of true randomness in human-based chosen complex passwords led many computer security experts to recommend very long passwords, which are very hard to remember. This led other experts to recommend easier-to-remember, even longer, more "natural" passphrases. They certainly will defeat today's password crackers, and that's a good thing. But, some programs have a 16-character limit on passwords (thank you Microsoft) so if Passphrases is truly the way to go, software makers will need to re-think their capability.

We will see if the industry does move towards a different approach to passwords. In the meantime, using two-factor authentication with complex passwords is still the best defense against the hackers. Call us for help with a password policy.

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. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Different Browsers for Privacy

Privacy is one of the hardest things to find today — and one of the most prized, especially online. Most people are concerned about the amount of personal information that is being harvested by governments, corporations, third-party agencies and/or unethical hackers. Many users are content to simply install a decent anti-malware application and hope their passwords remain secret. Others install personal VPNs.

But, those who are most concerned are moving from the more popular browsers – Chrome, Internet Explorer/Edge, Firefox and Safari – to special browsers that have been designed with the express purpose of preventing the collection of user data. The three that are best known are Epic, Brave and Tor.

Epic is a relatively new browser that has received postive reviews. It is based on the Chromium platform so it looks like Chrome. However, when installed it sets a high level of protection and it is up to the user to "downgrade" protection as needed, as opposed to most browsers that start at the minimum level and force you to increase your privacy settings. The browser blocks trackers and third-party cookies while keeping your searches from being tracked. If a specific site refuses to work because of the privacy tools, an icon to the right of the address bar pops up a window that allows you to quickly enable or disable whatever is causing the issue, such as a plug-in, encryption or ad blocking. It also links to a window that shows you which trackers and ads have been blocked.

Like Epic, Brave is based on the Chromium platform, and like Epic, it blocks ads and trackers. An icon on the toolbar lets you tweak features such as ad blocking, cookie control, and fingerprint control. Brave has two levels of anonymous browsing. 1) Private Tabs means that your browsing history, cookies and other footprints are not saved when you close the tabs. It also hides your IP address and location, and the sites you are visiting, from your ISP. 2)Private Tabs Using Tor, currently in beta, takes it one step further – it uses the Tor browser to send your site requests through intermediary relays to privatize your browsing.

The Tor Browser is the place to go if you're truly concerned about privacy. The Tor (short for "The Onion Router") Project is an open-source network formed to maintain browsing anonymity. It does this by using a volunteer-run distributed network of relays; each time you send a request to the Tor browser, that request will hit several relays before reaching its final destination. As a result, it is difficult or nearly impossible for a site or advertiser to track you online. It also means that some sites (such as Gmail) may ask for extra identification whenever you visit them via Tor, while others may reject the browser entirely.

So if on-line privacy is of utmost importance to you, you might wish to look at one of the alternative web browsers.

"Random Tid-Bytes"

Microsoft Extends Support

Microsoft has changed terms for Windows 10 support. Again. In February, it added six months to the usual 18 for each twice-annual feature upgrade, but declined to say whether the deal would be permanent or just a stopgap. Three months later, it became clear it was the latter when Microsoft said it wouldn't offer the same to April's upgrade. Now, Microsoft has backtracked and suddenly announced that support for Windows 10 would last 30 months. If you're running Windows 10 Home, Windows 10 Pro or Windows 10 Pro Workstation, the support calendar stays the same. But for customers running Windows 10 Enterprise or Windows 10 Education the schedule has again been altered. Microsoft gave its most important customers, whether commercial or academic, an extra 12 months of support for each already-issued Windows 10 feature upgrade. Rather than halt security and non-security updates to Windows 10 Enterprise and Windows 10 Education upgrades issued from August 2016 through April 2018 - after 18 months, Microsoft will instead provide 30 months of support for those versions.The 30 months of support decision takes effect immediately.

Office Users Get Reprieve, Too

Microsoft is giving Office 2016 a reprieve too, saying that the one-time-purchase suite will be allowed to connect to Microsoft's online services for three more years than ruled earlier. In April 2017, Microsoft proclaimed that applications provided by Office 2016 would be unable to connect to cloud-based Office 365 services after Oct. 13, 2020. The ban on accessing services like Microsoft-hosted Exchange inboxes, OneDrive storage space and Skype for Business' conferencing was part of sweeping changes to Office's support statutes – all part of a push to get more customers to adopt Office 365 subscriptions. Microsoft's statement said "To give you more time to transition fully to the cloud, we are now modifying that policy and will continue to support Office 2016 connections with the Office 365 services through October 2023."

Firefox Ends Support for Old Operating Systems

Mozilla has shut down Firefox's support for Windows XP and Windows Vista, ending browser security updates for the outdated operating systems. Support for the two past-expiration-date OSes - Microsoft dropped Windows XP in April 2014, Vista in April 2017 - ended with Firefox ESR 52.9, which was released June 26. That version was supplanted by Firefox ESR 60.2 on Sept. 4. Firefox ESR, for "Extended Support Release," is a version Mozilla issues to customers – primarily business users – who value stability over snazzy new features. Unlike the standard Firefox, each ESR version receives only security updates during its tenure. About once a year, Mozilla replaces the existing ESR with the then-current Firefox, then maintains both the old and new ESR versions during a 12-week overlap period. Firefox ESR 52's overlap with ESR 60 began May 7, when the latter launched, and ended Sept. 4, when that date's security patches were not provided for the former. Mozilla automatically moved Firefox users still running Windows XP or Vista to ESR 32 in March 2017; they have been browsing with that version since. Other browser makers – notably Google and Microsoft – removed Windows XP and Windows Vista from their support lists some time ago.

Windows 10 Tricks for Improved Performance

Microsoft Windows 10 has gone a long way towards fixing the problems that were found in earlier versions of Windows — notably Windows 8. Looking through various user discussions on tech blogs, there are six problems that a lot of people are complaining about: forced Windows 10 updates; lost disk space; sluggish boot times; annoying notifications; and problems with the Start menu.

If you are experiencing any of these problems, here are some tips to at least make them a little less irritating.

Get around forced Windows 10 updates

For many people, this is the biggest Windows 10 headache of all. Unlike earlier Windows versions, Windows 10 doesn't let you pick and choose which updates to install. Now when Microsoft issues an update, your machine installs it. However, Windows Update does give you some control over when updates will be installed, so they won't interrupt your work. And Windows 10 Professional, Enterprise and Education users can defer updates.

There are also a few workarounds that let anyone, even Windows 10 Home users, stop the updating process. (As a general rule, it's a good idea to keep Windows 10 current, because many updates don't just fix bugs or add new features, but also contain security patches.) However, it's your machines, so if you want to halt forced Windows 10 updates, there are ways to do it.

Windows 10's metered connection feature is designed to save you money if you pay for bandwidth use over a certain amount, but you can use it as a clever workaround to stop automatic updates. By default, this feature is turned off for Wi-Fi and Ethernet connections, but turned on for cellular data connections. From now on, Windows 10 won't automatically download and install updates. Or, you can go to **Administrative Tools/Services** and disable Automatic Updates there.

Recover lost storage space

Windows 10 can be a hard-drive hog, especially if you've upgraded to it from a previous version of Windows, or after a major Windows 10 update. That's because when you upgrade or install a major update, Windows 10 keeps the earlier version of the operating system, just in case you want to revert to it.

But that old operating system version is taking up several gigabytes of storage space. If you've got a PC with plenty of storage, no worries. But if you're stretched for storage, it can be a serious problem.

If you're sure you're not going to want to revert to your old version of Windows, you can easily delete it by using the Disk Cleanup tool:

1. Run the tool by typing **Disk Cleanup** in the search bar and clicking the Disk Cleanup search result that appears. The tool will take a few minutes to look through your system.

2. When Disk Cleanup has finished, scroll down the list of files you can clean up and check the box next to "Previous Windows installation(s)." This entry will only appear if you've got a previous Windows installation on your hard disk. Then click **OK**.

The old version of Windows will be deleted, and you'll get your hard disk space back.

Speed up Windows boot time

From the moment that Windows 10 was released, people started complaining that their boot times were more sluggish than with previous versions of Windows. Here are two ways to speed it up:

1. Enable Fast Startup – Windows 10 has a feature called Fast Startup, which combines a normal shutdown with the Windows hibernate feature. With Fast Startup, when you shut down your PC, it closes your applications and logs off all users, but loads the Windows kernel and drivers to a hibernation file on your hard disk. Then, when you restart your PC, Windows loads the kernel and drivers from the hibernation file, speeding up startup.

2. Use Task manager – with this, you can to disable programs that run on startup. Right-click the taskbar and select **Task Manager**. If the Task Manager runs as a small window and only shows the applications that are currently running on your system, click the "More details" link at the bottom of the screen. This opens up an expanded view, with multiple tabs across the top of the screen. Click the **Startup** tab. It lists all the applications that run on startup. Right-click each application you don't want to run on startup and select **Disable**. You'll still be able to run the program by launching it in the usual way — it just won't run on startup.

Turn off annoying notifications

The Windows 10 Action Center sends you notifications about your email, social media, software updates, system messages and much more. That can be useful or intensely annoying, depending on your personality and how many notifications you get.

There's an easy way, though, to turn off the notifications on an app-by-app basis, or to stop them all in one fell swoop:

1. Go to **Settings > System > Notifications** & actions.

2. To turn off all notifications, slide the button just under Notifications & actions to **Off**.

3. If you want to keep some notifications but not others, don't turn the slider to Off. Instead, go to the "Get Notifications from these senders" section and, next to any apps and services from which you don't want to get notifications, move the slider to Off.

Hopefully these tips will make your Windows 10 experience a bit better. Microsoft continues to "tweak" the operating system with the downloads that the company issues biannually, so while you might be tempted to turn off Automatic Updates, be sure to monitor when Microsoft does issue a major update as it is usually an important "fix" for Windows 10. Call SIM2K for more information.

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

Data Protection Tips

SIM2K often hears from clients saying that their "files are all stored in the Cloud" so they believe that their laptop does not need security as the data is all "up there." This is very problematic, especially for any employee in a regulated industry such as finance or healthcare.

We will pick on Dropbox for the purpose of illustration here. Yes, you can upload documents to Dropbox, and then be able to access them from any other device synced to your Dropbox account. But that little Dropbox folder on your laptop has a copy of each of those documents still right there on your hard drive. So, if your laptop were to be lost or stolen, the "bad guy" has your work right there in front of them.

There are some steps to take to help protect your data. For example, in Dropbox, you can go to the website dashboard for your account and activate **Selective Sync**. Here you can choose what folders are synced to your laptop. This way, you can keep confidential information on Dropbox, but that folder will not be mirrored on your hard drive. You then go to the Dropbox app to retrieve a document directly from the Cloud, and then up-load it right back to that folder when done.

Another recommendation for anyone wanting to protect the contents of their work, not just finance and healthcare, is to use the built-in disk encryption tool in Windows 10. Microsoft has built in BitLocker and it can be easily activated. This will encrypt your entire drive, so you will need to have a password to "unlock" data as you log into your Windows 10 account. If the device is stolen, the thief will not be able to view contents of the drive.

To activate BitLocker, go to **Control Panel** in Windows 10 and click on **BitLocker Drive Encryption**. Select the drive you wish to protect (i.e. C:). Then, at the bottom of the screen, click on **Turn on Bitlocker**.

You will then be taken to a screen where you will be asked to enter a password that will unlock the drive. **DO NOT FORGET THIS PASSWORD!** BitLocker now generates the encryption key. The next screen gives you the ability to back up the encryption key, either by making a copy on a USB stick, saving to your Microsoft Account or printing it. If you choose to use the print or USB options, put the key in a secure location - don't tape it to your keyboard.

Finally, BitLocker will ask if you want to encrypt just the "used" portion of your hard drive (the data on it) or the entire volume of the drive, which you may want to do on an older PC as "deleted" information is still on the drive and could be recovered. Once you finish this step, your data is now encrypted and cannot be read without the encryption key being activated. Call SIM2K for assistance in setting up BitLocker, or if you are running Windows 7, we can install BitLocker for you.

Scam Uses Your Password

A new twist on an old trick has emerged. The porn ransom e-mail claiming to have incriminating video of the recipient which will be released to contacts if not paid in bitcoin, has now included an old compromised password of the recipients in an attempt to add credibility to the scam. You have to appreciate the creativity here. By using your password the scammer hopes to scare you into action by giving the e-mail a sense of legitimacy. The typical e-mail reads like this:

I am aware, (Old, Compromised Password), is your password. You do not know me and you are probably thinking why you're getting this e mail, correct?

Actually, I setup a malware on the adult vids (porn material) web site and do you know what, you visited this site to have fun (you know what I mean). While you were watching videos, your web browser started working as a RDP (Remote control Desktop) that has a keylogger which gave me access to your screen and web camera. Right after that, my software program obtained every one of your contacts from your Messenger, FB, as well as email.

What exactly did I do? I made a double-screen video. First part shows the video you were viewing (you have a good taste lmao), and 2nd part shows the recording of your webcam.

exactly what should you do? Well, I believe, $1900 is a reasonable price for our little secret. You'll make the payment by Bitcoin

Note: You have one day in order to make the payment. (I have a specific pixel within this email, and now I know that you have read this message). If I do not receive the BitCoins, I will definitely send your video recording to all of your contacts including close relatives, colleagues, and so on. However, if I do get paid, I'll destroy the video immidiately. If you want evidence, reply with "Yes!" and I will send your video recording to your 13 friends. It's a non-negotiable offer, and so do not waste my personal time and yours by replying to this email.

The scam can be convincing because the password sent in the e-mail may be one of the recipient's actual current or former passwords. Security experts believe these were passwords that were compromised by a data breach, such as the Yahoo breach a year ago. Scammers know that people tend to re-use the same password on various sites, and can often link a person's password to an e-mail account, thus having this sextortion scam drop right into your inbox.

The password may be one that the recipient has used, but it's very unlikely that the scammer has actually installed any malware on your computer. While sextortion scams like this have been attempted for years, there are no reports of any scammers using this tactic and actually installing malware to film someone pleasuring themselves while watching porn. It's much easier to just lie about it and convince people that this has happened. And if you get this, and it does reveal a password you are using, you better change it on all sites immediately as you have confirmation your password is exposed. Call SIM2K if you need help here.