Expert IT Solutions Newsletter

Issue 11 October 2015

Welcome to another issue of our newsletter. This time we look at securing your work or home devices (laptops, desktops, tablets and smartphones) and new devices from Microsoft, the Surface Pro 4 and Surface Book.

Security checklist

Can I ask you one thing? Yes – you, reading this newsletter right now. Please read through the checklist below and take it to heart. If there are any actions in here that you are not doing today or weren't aware of, please do them and tell your co-workers and friends / family about them.

In our personal and professional lives we are more reliant on technology than ever and the sad truth is that very little of this infrastructure is actually secure or robust. In the quest for the latest, coolest feature /design in a highly competitive industry, both hardware and software is churned out with security is an afterthought, if it's even thought of at all.

In the last newsletter we looked at some high profile breaches of bigger businesses and organisations so we won't cover that here. I will however look at the threat actors that are out to get you and your data.

Hacking is now firmly in the domain of organised crime and other professionals. The software is developed just like legal software, bigger players have help desk support for their software and if a particular attack fails, some even have a "money back guarantee". And the return on investment is phenomenal. Recently I learnt that on average the return on Cryptolocker type attacks is 1,425%. That means a $ 5000 investment in tools and attacks will net you a bit over $ 70,000. Try getting that sort of return at your local bank!

So what are they after? They're after three things:

1. **Personal identification information**. Preferably account details and credit card numbers but anything, including your username and password has value, perhaps as a stepping stone for the next step in an attack or for blackmail or identity theft. As we become a more digital society this will start to include health information as well.
2. **Your business data**. Again, even for small businesses this has value on the black market.

3. **Your device**. If I "own" (successfully compromise) your device or server I can use it to attack other internet hosts (renting "bots" to others for attacks is big business). Or I can use it to send spam emails, or malicious emails with malware such as Cryptolocker to many thousands of innocent users. I can even use it to mine bitcoins, taking advantage of your processor to make money.

So how should you protect yourself and your business? This checklist doesn't cover every angle but aims to give you short, easy, actionable steps you can take today:

1. Keep your computers up to date. Not only Microsoft updates (Expert IT Solutions keeps tabs on your Windows business computers and servers) but other software such as Adobe Reader, Media players and other apps that you use on a day to day basis. Most apps provide a built in update feature, make sure it's turned on. Many attacks are successful because they exploit vulnerabilities where patches are available but people haven't installed them. Turn on Windows Update on every home computer you have and make sure to install every update it recommends.

2. Keep your Apples up to date. If you have Mac computers, make sure you update these as well. There's a persistent myth that Macs don't get viruses which isn't true. And the state of anti-malware software for Macs is not as good as on the Windows side. If you have Mac computers that need protection, contact us.

3. Keep your devices up to date. If you have Android or iOS tablets or phones, please update these. There are already lots of malware for Android and some really scary bugs (Stagefright comes to mind). iOS is less susceptible because of the tight control Apple keeps on the store but it's definitely not a given that you won't be attacked / infected, especially if you have a jailbroken device. If you need the ability to remotely wipe these devices, if they're lost or stolen, we recommend Microsoft Intune, contact us if you're interested.

4. Install AND keep up to date an antivirus / antimalware solution. Definitely on your Windows PCs (Expert IT Solutions maintains this for your work computers) and if you do banking or other sensitive tasks on your Android / iOS device, they should be protected as well. Be aware that even the best AV solutions today only catch 50-75% of malware, simply because the bad guys have automated ways of putting out slightly different versions, requiring the AV vendors to identify 1000's of different viruses every week and they can't keep up. Having AV is better than not but don't rely on it catching everything.

5. Turn on Windows Firewall, or the one supplied with your AV solution. We maintain this for your work computers. If a device is running a different OS but has similar protection features make sure to turn it on.

6. Don't open email attachments from people you don't know. And if you do know them and the attachment or the email looks suspicious, check with them first.

7. Not all cloud services are the same. Today it's popular to use Google Drive, DropBox, Box, iCloud, OneDrive and the like for storing your files in the cloud. Some of them scan your documents so they can serve you personalised advertising and if it's a free service, you can be absolutely sure that they offer no real guarantees that they won't lose your data to failures or malicious attacks. This doesn't mean you shouldn't use these services for personal documents (depending on how sensitive they are) but please don't use them for business

data without weighing up the risks (and checking with us).

8. Backup your data. Ideally you should have the original data on your server / device, a copy on site for fast recovery and one more copy off site for disaster recovery (not much point having the only backup sitting next to the server when the office burns down). This goes for your personal data as well, buy an external HDD and run a backup every night or a few times a week, depending on how much data you're willing to lose.

9. Don't share your password with others in the office. Don't share your personal passwords at home.

10. Change your passwords frequently. This limits the time someone can use your credentials to take actions "as you". On your business network you should be prompted to change your password regularly. For any personal sites that involves credit cards or banking details use good passwords. A "good" password is long and contains a mix of uppercase and lowercase characters along with numbers and symbols. I use passphrases such as "ILoveWorking@MyCompany@llDay-". Relatively easy to remember and very hard to crack (that's 29 characters right there).

11. Check if your business has any privacy obligations under Australian law, at http://www.oaic.gov.au/.

12. Notify us when someone leaves the business so we can disable their account. This is something that's checked during the monthly maintenance but it's best to disable their account as soon as they leave. If they're using any business cloud services, make sure you change the password for their accounts.

13. Put in a place an Acceptable Use Policy (AUP) for all staff. If you allow staff to use their computers with no restrictions you can be held responsible for the bullying of other staff or online harassment they do. An AUP outlines what's OK to do and what's not OK to do on company IT devices and emails / phones and when. (Perhaps checking Facebook is OK during lunch hours). If you'd like help putting together an AUP for your business, let us know.

14. Change the default password for your home router and / or Wi-Fi access point. Write it down somewhere so that you can find it if you need it at a later time.

15. Finally – update your home router. It turns out that the device that connects you to the internet through ADSL is really insecure (yes, all brands and models). And hacking it is really easy and can give the attacker access to all the devices on your network. Log on to the router with your new password (point 14) and on the left hand side (usually) it'll have an option for management / maintenance; pick backup. That'll let you save the setup of your router before you update. Then pick "update" which will download a "firmware update" for your router. Install this using the instructions in the router interface. Expert IT Solutions deals with the updates for your business ADSL router.

Please implement these 15 steps in your day to day life and make all of us a bit safer. And let us know if you have any other recommendations that we can put into the next newsletter to share.

Surface Pro 4 and Surface Book

As expected Microsoft announced the Surface Pro 4 (left) on the 6th of October but followed it up with an unexpected device, the Surface Book (right). The "Book" is a laptop but the screen is detachable and turns into a tablet.

Both will come in a variety of configurations with a maximum of 16 GB of memory and 1 TB of SSD storage. The Surface Pro 4 is exactly the same size as the Surface Pro 3 but the screen is bigger with the bezel being narrower. It's also lighter and thinner than Surface Pro 3. Both devices support Windows Hello, the new biometric login feature in Windows 10, which we'll cover in next month's newsletter.

On display was also two new Windows phones. The coolest feature here is "continuum", a Windows 10 feature that lets you take one of these phones and connect a keyboard, mouse and monitor to a very small docking device. Any Universal app (a program that's designed to run on Windows 10, whether on a tablet, desktop, Surface Hub collaboration 84" monitor or a Windows 10 smartphone) will scale to adopt to the screen size. And the phone still works as a phone and you can make calls whilst using it as a mini computer. So if you're looking for the ultimate in portable computing (as long as you have a screen and keyboard / mouse where you need it) these phones are it. Pretty cool.

To see the devices and the continuum demonstration check out the video here.

If you have any questions or suggestions for topics you'd like covered in this newsletter, please email us.

In the next newsletter we will look at the benefits of learning to write code and the Internet of Things (IoT).

If you no longer wish to receive this newsletter please email unsubscribe@expertitsolutions.com.au. If you have colleagues, friends or relatives that could benefit from this newsletter, please ask them to email subscribe@expertitsolutions.com.au.