PASSWORDS ARE LIKE UNDERWEAR - WHY YOU SHOULD CHANGE THEM OFTEN.

An e-book on cyber security and awareness – how not to get scammed.

www.ispcomputers.ca

ISP COMPUTERS

ABOUT ISP COMPUTERS

We've all experienced it. "Computer betrayal", that unexpected, unexplained cessation of all user-friendly behaviour on the part of your PC, usually in the middle of a project, in the middle of the night, the night before a crucial "do it or you'll be deadline".

OK, not a nuclear disaster, but it can sure feel that devastating!

Times have changed. We've become completely dependent on our data devices. The modern world cries out for a new breed of superheroes. They are ISP Computers - your top technology solution!

Together, Jodi Fulford, business manager and their computer customizing league of "OS stressbusters", featuring husband, Iain, champion of corporate clients, and oracle of all that is IT, they've created a safe, engaging computer "community" that's your first choice for quality products, reliable repair, and relevant, researched computer education.

"ISP stands for what we are, an "Interactive Social Place" to help you feel "Involved, Supported and Positive" about technological "Information, Service and Products."

ISP Computers, your IT Success Partner.

Jodi Fulford
Business Manager & Geek Speak to Human Translator
780 - 960-2150

ISP Computers Ltd.
Since 2004
#204- 205 Jennifer Heil Way
Spruce Grove, AB. T7X 0T3
rma@ispcomputers.ca
www.ispcomputers.ca

PASSWORDS ARE LIKE UNDERWEAR – WHY YOU SHOULD CHANGE THEM OFTEN

Modern day Pirates are on the attack. But instead of the loot and the booty of treasures, they are making your computer data and your credit card payments their prey. In the midst of the age of technology, many people are left floundering about how their machines work, are trying to decode multiple devices and are having to comprehend concepts such as cloud storage and syncing. And the pirates are taking advantage of this confusion.

The method most used is the scare tactic, where an alert or email implies that your machine is going to blow up at any minute. Within the confusion you get offered an easy out – download this software, run this program or phone now to help. Because of hard sales practices, you aren't given the chance to say no once you have made contact and the pirate takes advantage of your trust and unawareness, while blind. And it gets worse from there.

Don't take tech advice from strangers. Call your community computer center.

THE HARD TRUTHS

On Thursday, March 31, 2016, the United States and Canada issued a rare joint cyber alert, warning against a recent surge in extortion attacks that infect computers with viruses known as "ransomware", which encrypt data and demand payments in order for it to be unlocked.

The warning follows reports from several private security firms that they expect the crisis to worsen, because hackers are getting more sophisticated and few businesses have adopted proper se-

curity measures to thwart such attacks.

“Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist,” the two governments said in the alert, distributed by the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre.

It comes in the wake of reports of a string of ransomware attacks on individuals, businesses and government agencies in the past few months, including some that interrupted services at U.S. hospitals and police departments.

A recent report from Intel Security’s McAfee Labs found that ransomware attacks have more than doubled in the past year. The internet security firm estimates that ransomware is now earning criminals $10 million to $50 million a month.

What do cyber criminals get?

- Payment Card Numbers & Data (approximately 84%)
- Authentication Credentials (approximately 84%)
- Copyright & Trademarked Materials (approximately 75%)
- Medical Records (approximately 73%)
- Classified Information (approximately 72%)
- Bank Account Number & Data (approximately 70%)
- Personal Information (approximately 60%)

Stats: http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-19-en.aspx

So, what is Ransomeware?

It is a form of malware or malicious software. The dangerous software usually comes in the form of a spam email, which is being sent in the form of an invoice, a website or video. When the computer user opens the attachment, the software then gets to work encrypting all of the data on the user's computer. By encrypting the data it locks out the user, making the data inaccessible to the computer user.

There are two main sorts of ransomware:

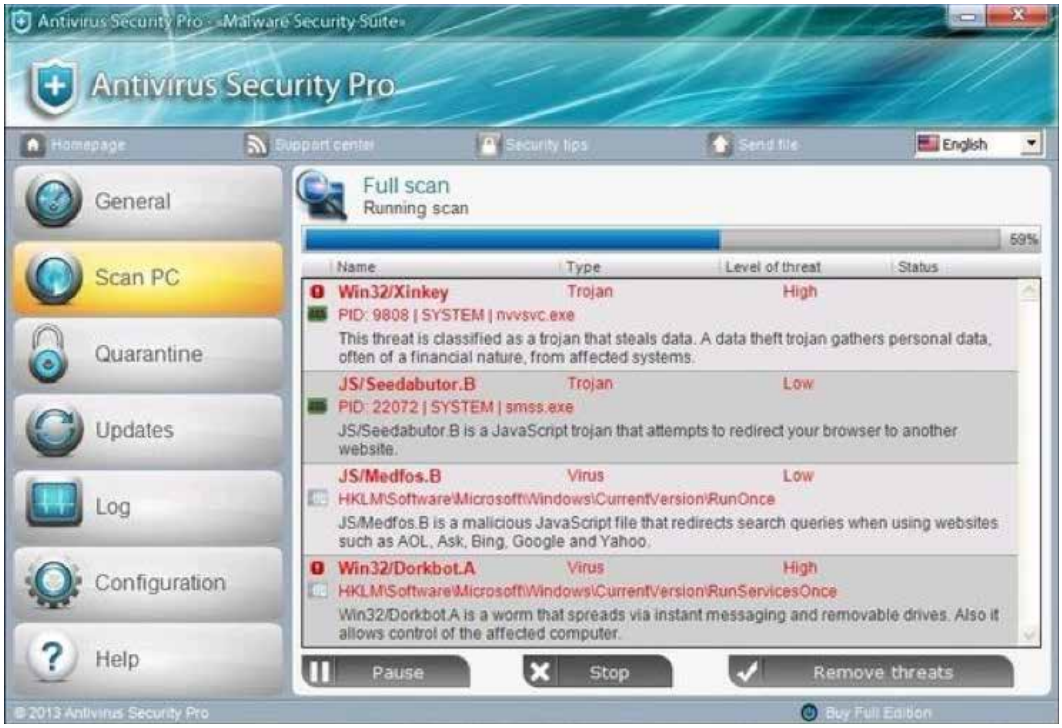
- **Lockscreen ransomware** pops up a window that takes over your computer or mobile device, so you can't use any other applications, make calls, or run your anti-virus. This ransomware usually accuses you of some sort of crime, but offers to let you keep on working once you have paid a "fine."
- **File-encrypting ransomware** leaves your applications running just fine, but scrambles your data files so you can't open them any more. This ransomware usually pops up a window offering to sell you the decryption key.

Most often, the files targeted by ransomware are photos, videos and business records like spreadsheets, documents and presentations — anything likely to be valuable to a person, family or business.

In order to regain access to the files on the computer, the user is forced to pay a ransom. The ransom is usually requested in Bitcoin, which cannot be traced. However, there is no guarantee that paying the ransom will see the data on the machine unlocked.

What do they look like?

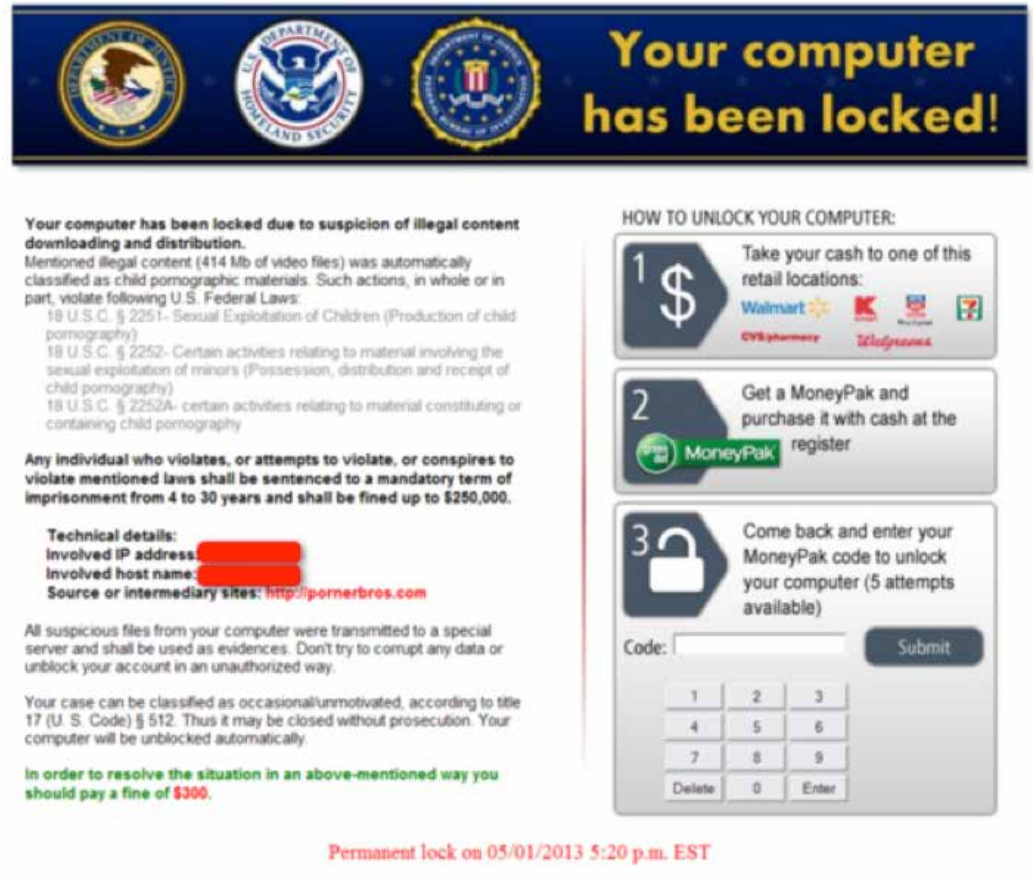
The simplest type of ransomware, aka scareware, consists of bogus antivirus or clean-up tools that claim they've detected umpteen issues, and demand that you pay in order to fix them. Some specimens of this variety of ransomware may allow you to use your PC but bombard you with alerts and pop-ups, while others might prevent you from running any programs at all. Typically these invaders are the easiest type of ransomware to remove.



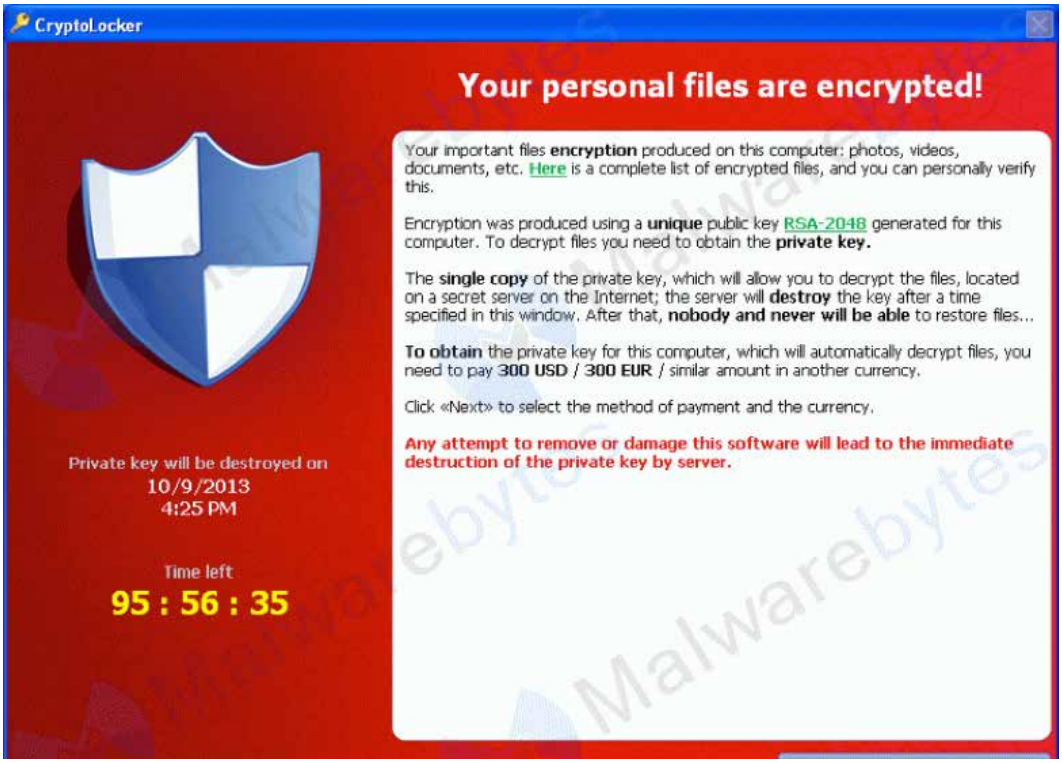
An example of a fake antivirus app.

Next is the ransomware variety that is called lock-screen virus, which doesn't allow you to use your PC in any way. It displays a full-size window after Windows starts up—usually with an FBI or Department of Justice logo—saying that you violated the law and that you must pay a fine.

The Kovter ransomware locks down your computer, displaying a fake notice claiming to be from several government authorities.



CryptoLocker spreads via .zip files sent as email attachments, for example.



How does your computer become infected?

Your computer is typically infected with malware such as ransomware when you open an attachment to an email or download software or apps. Such emails and software can appear legitimate enough to fool many users. Pops ups in the form of the images above – urge you to call what seem like legitimate companies. They ask you to install a program that allows them access. Downloading harmful programs, whether intentionally or not, can allow viruses or even users from other countries access to your data. All of these scenarios can lead to loss of money, time and data.

Signs that your machine is infected:

- Your system shuts down spontaneously and frequently, even if you don't use it.
- Your Internet connection slows to a crawl even while you are not doing anything significant.
- Your virus scanner crashes and cannot be started again.
- You are no longer able to visit antivirus sites.
- Your hard disk fills up and you can't find the files that use up all the disk space.
- Your computer seems to be displaying an inability to start (boot up) or taking longer than normal to start up.
- Your computer is exhibiting unpredictable program behavior.
- Strange graphics appear on your screen.
- A complete inability to access any program or data.

How can you protect yourself from ransomware?

Security and Prevention

- Antivirus and malware protection: Antivirus software is one of the most important tools for safeguarding your computer, vital information, and personal data from the daily onslaught of viruses and worms. Without antivirus protection, your computer may be left completely defenseless against perpetrators' relentless attempts.

- Once you have your **antivirus**, ensure that it is up to date. Missing even one daily update can make you vulnerable because the **malware** keeps changing. Don't open attachments or download software (often free programs or games to your computer or phone) that you can't be sure are safe.

DID YOU KNOW?

An antivirus and malware program can run simultaneously on your computer and protect you from different attacks. However, if you are running more than one antivirus program – they will attack each other leaving your computer vulnerable to virus infections.

- Perform daily scans: Remember, your virus protection is only as effective as its last update. New viruses appear all the time (Norton and McAfee experts estimate that there are currently more than 50,000 viruses in existence and approximately 200 discovered each month). If your **antivirus** software isn't current, the latest viruses or worms can sneak in.
- Back up - It's a good idea to backup all your files on a hard drive that is not connected to your computer so that you have a clean and accessible copy of your files if your computer does become infected. Remember: if you don't have backups and you lose your laptop, you're in the same trouble – worse, actually – than you would be with ransomware.
- Be aware of PEBKAC – Problem Exists Between Keyboard And Chair. Most viruses are installed because of human error and complacency. The word 'FREE' can cost you in the end.

TIP: PASSWORDS ARE LIKE UNDERPANTS

1. Keep it to yourself – don't allow others access.
2. Change them often – at a bare minimum once a year, please. You can do it right now.
3. Don't leave them out where anyone can see them – don't hit 'remember me' when your browser offers.

Education at the office

- Educate your staff on cyber security. Talk about phishing and social media scams. Have clear internet usage policies.
- Establish policies for using email safely. Separate work and personal. Stop opening attachments from people you don't know.
- Know what you are allowing on to your computer. Freeware and shareware programs often come bundled with spyware, adware or fake anti-virus programs. Don't install programs that you don't know, aren't using for work or that someone (other than your IT technician) has asked you to install.

Tip: When installing a program you are given the option of choosing an automatic or a custom install. If you are installing something from the Internet we suggest doing a custom install to make sure nothing else is added or changed during the install.

Think you are too small?

- 90% of small businesses believe a cyber attack would have serious impact.
- 50% of small businesses don't think that they're targets of cyber crime.
- 40% of all cyber attacks in 2011 were on small to medium sized businesses.

Stats: Symantec SMB Threat Awareness Poll Global Results, September 2011

What happens if you pay the ransom?

Now, there is no guarantee that you will get your files back if you pay. So in theory – here's how it should work:

If you pay the ransom, the cybercriminal provides a code, which triggers the decryption process. That can take days or weeks. Once files are decrypted, you'll be able to access them again.

Did you know? The governments discouraged victims from paying hackers to restore access to their data. “Paying the ransom does not guarantee the encrypted files will be released,” the alert said. “It only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information.”

Should you pay the ransom?

So the big question, usually left unanswered in technical discussions of ransomware, is, “Should you pay?”

At a typical cost of $900 to $2000, ransomware can be expensive.

On the other hand, think about what might be in those scrambled files: your baby videos; those tax return documents you were supposed to keep for seven years; the dissertation you need to turn in on Friday…how much are those worth?

For better or for worse, most ransomware gangs have acquired a bit of an “honour among thieves” reputation, so that if you do pay over the money, you almost certainly will get your files back.

On the other hand, law enforcement and security experts are very likely to say, “These are crooks! This is extortion! If you can possibly take it on the chin, we urge you NOT TO PAY!”

But those are easy words to say if it’s not your data on the line.

SUMMARY

In 2015, a ransomware campaign using a virus called Cryptowall 3 collected more than $325 million U.S. in ransom payments(that's one campaign, one year). As of April of this year, Computer security researcher McAfee has named ransomware as one of the biggest security threats of 2016. Locky and Cerber are two of the most prevalent and dangerous ransomwares currently active.

Ransomware is surging to a fever pitch, attacking personal home computers and businesses alike. It's one that will affect consumers and businesses equally as the criminals behind the malicious software don't care who the virus infects as long as people are paying their ransoms.

According to the researcher there were more than four million samples of Ransomware floating around on the Internet last year, more than 1.2 million of those samples were new. So to wrap this up: this ransomware is bad, but infection is preventable!

GLOSSARY OF TERMS

Antivirus software designed to detect and destroy computer viruses.

Bitcoin is a digital asset and a payment system invented by Satoshi Nakamoto.

CryptoLocker is a ransomware Trojan which targeted computers running Microsoft Windows, believed to have first been posted to the Internet on 5 September 2013

Malware is an umbrella term used to refer to variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software

- **Adware** – software that automatically displays or downloads when the user is online, typically pop-ups.
- **Freeware** – Copyrighted computer software which is free of use for an unlimited time.
- **Scareware** – Malicious computer program designed to trick or scare the user into downloading unnecessary software.
- **Spyware** – Software that is installed or downloaded into the user's computer to secretly obtain information about the user and transmit it back to advertisers or other interested parties.

Phishing (scams) – is the attempt to obtain personal information and/or banking by false websites pretending to be trustworthy business or institution.

Spam mail – unsolicited messages sent vial email. Theses emails are generally random advertising, otherwise known as junk mail.