SORT I.T. COMPUTER SERVICES NEWSLETTER

Issue 4 – June 2014

WELCOME

It's been over 6 months since our last newsletter. Being a small business we are lucky to get some 'quiet time' to get the newsletters out, but we still apologise for the delay. Winter is here and I hope that everyone is coping with the grey days and chilly times that it brings. With this in mind that I advise you that **Sort I.T. will be closed from 07/08/14 until 10/09/14**, as my family will be heading away for a Northern Hemisphere summer break to catch up with UK family and friends. If you have any urgent problems that you have been meaning to contact us with, get in touch during July, that way we can ensure that the problems are fixed in time.

We would like to welcome any new subscribers to this newsletter and encourage you all to get any friends and family to also sign up so that the information and education about computing grows.

Thank you.

Jason John
Sort I.T. Computer Services.

PASSWORDS

Here are the 15 most popular passwords used in 2013. If a password you use is listed below we suggest changing it:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. sunshine
13. 1234567890
14. letmein
15. photoshop

What password should I chose? The Only Secure Password Is the One You Can't Remember….

Let's assume you log onto a bunch of different websites; Facebook, Gmail, Trade Me, PayPal, probably some banking and much more. Consider a couple of questions:

- Do you always create unique passwords such that you never use the same one twice? Ever?
- Do your passwords always use different character types such as uppercase and lowercase letters, numbers and punctuation? Are they "strong"?

If you can't answer "yes" to both these questions, you've got yourself a problem. But the thing is, there is simply no way you can remember all your unique, strong passwords.

Passwords are the key to many systems and applications. Your password helps to prove who you are, ensure your privacy, and protect the privacy of data you may have access to.

Compromised passwords are one of the means by which unauthorized people gain access to a system. Someone logging on under your name has access not only to your computer files, but may also have access to your personal information (e.g. benefits, bank information) and may impersonate you to send malicious e-mail.

Many times you are requested to choose and maintain a password for various purposes (e.g. sign on to a file server, access your e-mail, use a password protected screensaver).

It's important to choose a strong password and protect it since there are many password-cracking programs readily available on the Internet and passwords are the key to access many computer systems or applications. A strong password makes it reasonably difficult to guess the password in a short period of time either through human guessing or the use of automated password cracking programs.

Choosing a Strong Password

The following are general recommendations for creating a Strong Password:

A Strong Password should

Be at least 8 characters in length

Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)

Have at least one numerical characters (e.g. 0-9)

Have at least one special character (e.g. ~ ! @ # $ % ^ & * ( ) - _ + =)

A Strong Password should not

Spell a word or series of words that can be found in a standard dictionary

Spell a word with a number added to the beginning and/or the end

Be based on any personal information such as user id, family name, pet, birthday, etc.

Be based on a keyboard pattern (e.g. qwerty) or duplicate characters (e.g. aabbccdd)

Use a passphrase or a nonsensical word

A passphrase could be a lyric from a song or a favorite quote. An example of a strong passphrase is “Superman is $uper str0ng!”. A nonsensical word can built using the first letter from each word in a phrase (e.g. C$200wpG., represents "Collect $200 when passing Go."). These typically have additional benefits such as being longer and easier to remember.

It’s not a bad idea to keep a book with your passwords in them, that way you can change them for different logins. If the book is ever compromised, you know that the sites that you use will need their logins changed. **It’s strongly recommended that your bank passwords are not included in this book!**

Finally, passwords are confidential. DO NOT GIVE YOUR PASSWORD TO ANYONE!

Still running Windows® XP?

The Windows XP operating system is no longer supported by Microsoft. If you continue to run XP then you are vulnerable to security threats. Now is the time to upgrade and this is why....

Known vulnerabilities will no longer be fixed

Since April 8 updates to Windows XP are no longer provided by Microsoft to fix known vulnerabilities. Similar to leaving your front door unlocked to burglars, hackers can now exploit new vulnerabilities found in XP because they know Microsoft is no longer proactively fixing them.

Your Internet browser and device drivers that enable the proper operation of your system will also be left behind. There is one particularly troubling security problem for an outdated version of Internet Explorer that runs on Windows XP (v8.0) that allows malicious software to enter your PC and gives the author full control of that system. Hackers use this vulnerability to install the "RAT Poison Ivy" software which gives them even more control of a single PC, and access to other systems.

Legal liability is a possibility

If you continue to use Windows XP in your office then you may be putting your client's data at risk. Some lawyers postulate that leaving these outdated systems in use might constitute negligence on the part of the organisation. One of the most common elements that impacts liability for data loss is the concept of "reasonableness." In other words, what is a reasonable and prudent set of actions to protect someone's private information and data? This is where ignoring the advice of the manufacturer and running outdated software such as Windows XP presents a very real potential vulnerability.

Software that runs on XP is also outdated

The security tools and software needed created by other software vendors (not Microsoft) to protect Windows XP PCs will also be discontinued, if not already. Key security software vendors such as Symantec, McAfee, and Trend Micro have already announced that they are ceasing or dramatically cutting back their support for Windows XP. Existing security software may run but without the updated virus signatures and technology to stop the latest threats Windows XP systems may end up effectively "defenceless".

If you would like additional information or have any other questions, please contact us at contact@sortitcomputers.com.