Security Threats

Know your foe

SHEEVAWN HILL

INTRODUCTION

Threats

- Malware
- Ransomware
- Phishing Scams
- Spyware

Threats and Remedies

The internet is very useful, but it also attracts con artists and tricksters from all over the world.

Learn to identify common online security threats – and keep them at bay.

Malware

Malware

What is it? The common term used for PC infections and viruses. It covers digital nasties and their many subsets, including trojans, viruses and worms.

How does it work? Malware can target your personal details or turn your PC into a botnet robot for spammers.

How do I beat it? Use good internet security software (anti-virus) and – keep it up to date so it can counter the latest threats.

VIRUSES

Attach to a program or file and require human action to spread from one computer to another.

WORMS

Can replicate inside a system and do not require human action to spread. (example – address list)

TROJAN HORSES

Appear useful but damage systems and require human action to run, do not self-replicate (Backdoor or DoS)

Ransomware

Ransomware

What is it? Software used to take over and lock a PC - and then charge for its return. It can encrypt all the files.

How does it work? Visiting an infected site or opening an infected email attachment can attract ransomware.

How do I beat it? Regular backing up of the PC with several versions saved will reduce ransomware to an empty threat.

Phishing scams

Phishing scams

What is it? Attempts by fraudsters to gain personal information, such as bank or credit card details or passwords, by posing as respectable parties.

How does it work? Victims receive an email that appears genuine and includes a link to a rogue site. The victim is encouraged to enter sensitive details which are then captured by the scammers.

How do I beat it? Reputable companies will never request a sign-in via an email link, so be suspicious of any email that does. You can hover your mouse over a link – without clicking – to preview the associated destination web address.

Spyware

Spyware

What is it? Software that spies and reports on your personal information.

How does it work? Typically Spyware monitors online activity and reports to third parties without your knowledge. It can slow down your PC/Mac

How do I beat it? Internet Security packages now include Spyware protection. Microsoft also provides a free scan and removal tool called Microsoft Safety Scanner. Beware of scams that offer to scan your PC, report infections and charge a fee to fix the issues.

SOLUTIONS

- Keep your device up-to-date
- Use security software
- Activate two-step verification
- Use ‘passphrases’, not passwords
- Don’t use one password everywhere
- Don’t give personal details away
- Know your online scams
- Avoid spam emails
- Never believe that Microsoft or Apple (iCloud) are phoning
- Think twice before tagging a location

Keep your PC up-to-date

- The latest versions of any software and virus scanners are generally more secure against online threats.

- Most packages can update themselves automatically.

  The update status can be checked on the internet via the package version or settings.

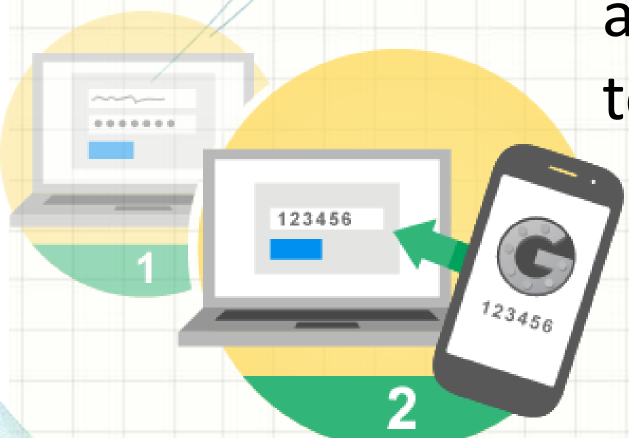
Use security software

- Install reputable security software on a PC.
- Anti-virus software protects you from viruses but Internet Security software protects you from other forms of malicious content such as a banking threats, dodgy websites, scams, spyware, phishing and ransomware attacks and other internet threats
- This should protect against 99.9% (if not 100%) of threats.

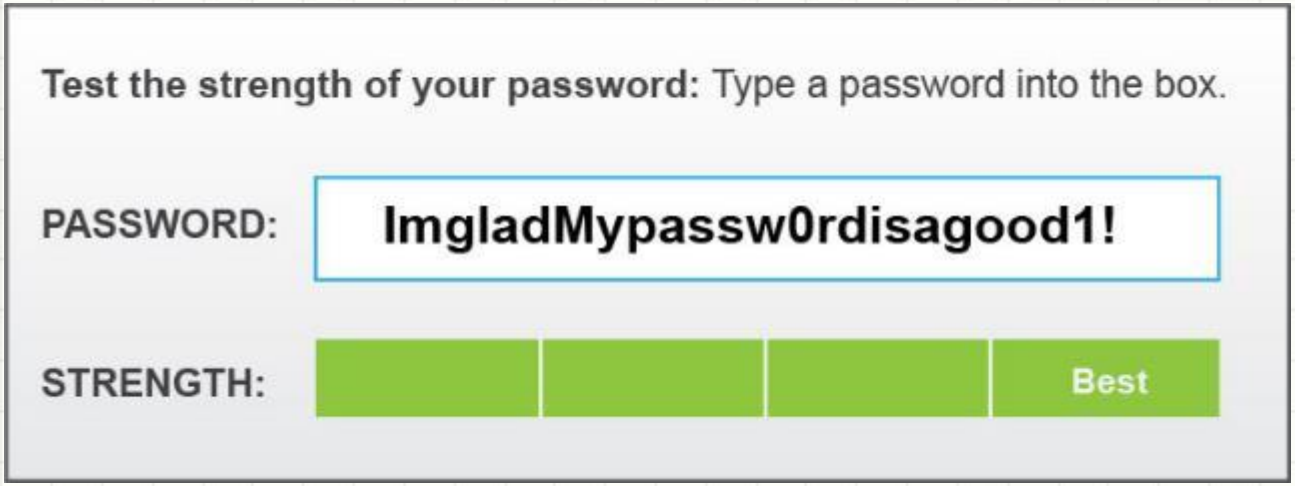
Activate two-step verification

Two-step verification adds an extra layer of password protection when using systems such as Gmail, Twitter and Facebook from a new device or location.

It introduces another verification step via a phone text message and prevents access to the accounts with just a password.



Use ‘passphrases’, not passwords



Test the strength of your password: Type a password into the box.

PASSWORD: **ImgladMypassw0rdisagood1!**

STRENGTH: Best

A passphrase is much more secure than a single word as it combines words, numbers and symbols for added security.

The idea is that hacking software will have a much more difficult task of deciphering a combination of words.

Don’t use one password everywhere

Much as it is less secure for a house, garden shed, garage and car to all open with the same key; the same applies to PC accounts and associated passwords.

I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything

Don’t give personal details away

Phone numbers today have become more personal. Do not publish them or other details such as email addresses on online chat rooms or message boards without considering the consequences.

Know your online scams

Be aware of the current threats being used to obtain personal information and money.

Avoid spam emails

Production and distribution of spam emails will never stop.

The best remedy is identification and application of tools and filters to capture and delete spam.

Never believe that Microsoft or Apple are phoning

A common scam is a call from somebody claiming to work for Microsoft or Apple or BT. They will announce that your PC or router is at risk and they require a remote logon to help secure it.

Don't believe them. Microsoft or any other reputable software provider will never make an unsolicited call and request this information.

Think twice before tagging a location

It is fun to let friends know about a holiday in a nice remote place but be aware that someone unintended may identify this status and assess the absence from home during this period.

WHAT CAN BE DONE?

- **UPDATES** are very important although, if you can – it is a good idea to wait a few days for any problems to be resolved
- **BACKUP** your most important information, and save in a secure location in case anything goes wrong with your computer.
- Install reputable **INTERNET SECURITY SOFTWARE** on both your Windows PC and Apple MAC.

QUESTIONS?

Sheevawn Hill
OrbitTech Limited
www.OrbitTech.co.uk
Telephone: 01932 300360