soVision IT

Protecting you & your business from Malware

www.sovisionit.com

soVision IT

What is Malware?

Malware, short for **malicious software**, is any software used to **disrupt** computer operations, gather sensitive information, gain **access to private** computer systems or display **unwanted** advertising.

Malware may be stealthy, intended to **steal** information or **spy** on computer users for an extended period without their knowledge or it may be designed to cause **harm**, often **as sabotage** or to **extort** payment (Crypto Locker).

Common Sources of Malware

- **Social Media Scams**
- **email Attachment Scams**
- **Videos Containing Malware**
- **Fake websites**
- **Click Through Advertising**
- **Browsing Deeply in Search Engine Results**
- **Scare Ware Pop Ups**
- **Urgent Call to Action Pop Ups**
- **Shared Videos and Links From Friends**
- **Outdated Anti Virus or Windows Updates**

How to avoid this? First step: **COMMUNICATION!**

Warn everybody of these attacks! Feel free to **send and share** this document explaining possible threats and warning people on how to avoid them or what to do once infected.

soVision IT

DANGEROUS NEW VIRUS
Crypto Locker

Crypto Locker is a virus that can easily pass through any antivirus and **encrypts Office or database files** on your local computer as well as the ones on the network.

Prevention:

- Be very careful in opening up **any attachment** particularly if it is linked to a FedEx or UPS shipping notice or a Banking email.
- Implement an **Application Control Policy** to limit the effect of the attempted attack.

Once infected, you will get a popup saying your files are encrypted and demanding a **ransom** to get them back. **Be Aware! The only recovery** is to restore from backup.

soVision IT

Impersonating websites

Keep a look-out for **fraudulent** websites that impersonate legitimate websites. Normally it's easy to notice the **poor grammar**, **certificate warnings** and **broken links**.

Most common ways of stumbling on an impersonating website is **falling for a scam**, either on a Social Media site or in an e-mail. It's also common to find them in a deep search listing.

> **Recommendation: Always pay attention to the URL in the address bar! If it doesn't relate to domain of the website, it's highly likely that it's an impersonation!**

Getting Lost in Deep Search Engine Results

When you search a subject, deep searching of results to find answers may not be a good thing! The deeper you go, the more you'll find **pages un-related** to your initial result, making a **higher risk** of accessing an **infected website**.

> **TIP: They are easy to detect as most of the time they do not make sense and its title and description is entirely unrelated to your initial search. Use common sense!**

soVision IT

Social Media Scams

Everyone uses social media today, making it a playground for scammers.

These scams can lead to anything! **Compromised accounts, malware, fraud** or **e-mail spam**.

How to avoid SM Scams:

- **Don’t trust a post, message, or invite just because it comes from a friend**.
- **Do a search to check out whether if something is valid before sharing it.**
- **Be very suspicious of offers for free stuff**.
- **Don’t follow links that accompany some hysterical or generic text.**
- **Avoid links that promise some current event “scoop”.**
- **Never click on a link to an app that promises a functionality.**
- **Don’t fall for chain “sharing”.**

soVision IT

Outdated Anti Virus or Windows Updates

Keeping your antivirus and operating system up-to-date should be **a top priority**. You should download updates as soon as you are notified of them or set your computer to automatically do this for you.

Why is this so important?

- There are literally **thousands of new internet threats** released in the "wild" every week. Your antivirus database need to be updated in order to keep on top of these new risks.
- **Hackers get smarter** each and every day, discovering new ways to gain access to your computer. Windows recognizes these security breaches and immediately releases a patch to prevent this from happening to you. Failure to update keeps your entire data vulnerable.

Recommendation: **Don't stop here!** You should **always update any software** on your computer that prompts you. Whether it's your Adobe Flash Player or Java Applet, you'll be amazed how easily hackers can get access to your system through security breaches of these tools.

soVision IT

Scareware Pop Up Windows

The most common way that a virus gets installed onto a system is by scaring you that something is wrong with your computer, **tricking you** to download or buy its product to “fix it”.

Prevention:

- Nothing can detect that you have a virus on your system EXCEPT for the **antivirus software running on your computer**! Keep it updated!
- If you suppose a “Scareware” popped up, **do not interact with the window.** Even clicking the “X”, it is coded to silently install it’s malware on your computer. To avoid this, shut down your computer instead.
- **Do not scan your computer for registry errors.** It will not improve system performance or make it faster. This is a very popular tactic to install malware on your computer by the large volume of fake software available.
- Windows Security Center is not an antivirus, if you get a “virus” notification from it, **don’t interact and do a virus scan immediately with your antivirus!**

soVision IT

email & Spam Scams

This is a very popular approach for foreign agencies to **install malware** on your computer or commit fraud.

It's easy to avoid., it's spam.

- If an e-mail comes in with no subject and a single link, with poor grammar, from an unknown person, it's a scam. **Simply delete and forget**!
- But what if it comes from a friend? How do you know if it's legitimate? **Call them and ask!**

YouTube Scams

YouTube videos claiming to be a full movie or your favorite show may ask to refer to a link in the description to see the full thing, only to find a website full of surveys to fill out.

By the end of it, your inbox is full of spam and your computer is full of malware.

Prevention:

- **Don't search for free movies or full TV episodes on YouTube!** They don't exist because it's illegal without discretion for them to be uploaded and it's also against YouTube's ToS.
- **Don't click on breaking news stories** or just about anything that will get a lot attention**. Always look at the ratings before you click on the video.** Normally the fake videos are rated very low.

soVision IT

What are you risking when unprotected?

- Malware can damage you personally
- They can cause harm to your friends and family
- They can damage your organisation
- They can cause significant cost in terms of professional support to rectify infected infrastructures and lost time, sales income and customer contact

Always be ALERT

If in DOUBT call your professional support team

As a last resort switch off and get HELP

soVision IT

Don’t give Malware a chance!

Prevention is the best protection!

soVision IT provides complete IT Security Services including:

- IT Security Audit & Penetration Testing
- Managed Antivirus
- Antispam Services
- Content Filtering
- Multifactor Authentication
- Endpoint Security & Data risk management
- Cyber Essentials Certification
- Secure Data Backup
- Remote & Online Backup Solutions
- IT Disaster Recovery Solutions

Contact us on 0117 986 4026 or at info@sovisionit.com

CYBER ESSENTIALS

AVG Gold Reseller

soVision IT

Secure yourself and your business before it's too late!

Complete ICT Solutions