What is Computer Security?

Ransomware is a type of malicious programme that demands payment after launching a cyber attack on a computer system. This type of malware has become increasingly popular among criminals, costing organisations millions each year.

For a quick guide to ransomware and what you can do to protect your business, download our free infographic: What is ransomware and how can I protect my business?

The impact of Cyber Crime

Security experts recognise that ransomware is one of the fastest-growing forms of cyber attack. Its prevalence and reach was emphasised when WannaCry, and more recently, NotPetya, exploited a flaw in Microsoft’s SMB software and spread rapidly across networks, locking away files. According to Bitdefender Labs, there are roughly 2.8 million known unique samples of ransomware and the numbers keep growing. DIY ransomware creation tools are also readily available.

How to protect your business in 30 minutes

Preventing ransomware attacks can be as simple as ten minutes of staff training. We’ve developed a Human Patch e-learning course to help you take action against the increasing threat of phishing and ransomware attacks by educating your employees to be vigilant and secure.

Protect yourself with IT Governance cyber security and technical services

IT Governance’s cyber security consultancy and technical services are delivered by a team of experienced in-house consultants and penetration testers who have a deep understanding of the range of cyber risks faced by organisations today, enabling you to implement the best possible security solutions for your budget and requirements.

Malware

Malware is a broad term used to describe any file or programme intended to harm a computer, and encompasses trojans, social engineering, worms, viruses and spyware.

Social engineering

Social engineering is used to deceive and manipulate victims to gain computer access. This is achieved by tricking users into clicking malicious links or by physically gaining access to a computer through deception.

Outdated software

The use of outdated (unpatched) software (e.g. Microsoft XP0 opens up opportunities for criminal hackers to take advantage of known vulnerabilities that can bring entire systems down.

Vulnerabilities in web applications and networks

Cyber criminals are constantly identifying new vulnerabilities in systems, networks or applications to exploit. These activities are conducted via automated attacks and can affect anyone, anywhere.

Penetration testing is an effective way to identify and eliminate vulnerabilities

While technical security measures continue to improve, phishing remains one of the cheapest and easiest ways for cyber criminals to gain access to sensitive information.

They might also compromise their personal information, login credentials such as usernames and passwords, and financial information, including credit card numbers.

This page provides an overview of phishing and explains how security awareness training can help you avoid falling victim.

What is Phishing?

Phishing is a type of social engineering attack in which cyber criminals trick victims into handing over sensitive information or installing malware.

More often than not they do this via malicious emails that appear to be from trusted senders, but sometimes use other means, which are explained below.