CYBER ALERT

# RANSOMWARE ATTACKS

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

VISIT SCOTLAND.POLICE.UK/KEEP-SAFE/KEEP-SECURE-ONLINE/
FOR INFORMATION ON HOW TO BEAT THE FRAUDSTERS

# Cyber Alert – Ransomware Attacks

**Ransomware (or ransom malware) is malicious software (virus) designed to block access to a computer system until a sum of money is paid to criminals behind the attack. Typically users are prevented from accessing their system, personal files or entire business network. Any consumer or business can be a victim of ransomware, as Cybercriminals are not selective often looking to hit as many users as possible for the highest profit.**

There are various ways in which ransomware can infect your computer or systems:

1. A ransomware attack is usually delivered via an e-mail attachment or link, often disguised in an email pretending to be from a well-known brand or contact. Once the attachment is opened, the malware is released into the user's system. Cybercriminals can also plant the malware on websites, when a user visits the site unknowingly, the malware is released into the system.

2. The malware is not immediately apparent to the user, and operates silently in the background until it has been successfully deployed onto the system. Then a dialogue box appears that tells the user the data has been locked and demands a ransom to unlock it again. By then it is often too late to save the data through any security measures.

3. Another method is through malicious advertising links that again send you to a fake website injecting malware onto your systems.

4. Scareware – usually pops up when you're browsing the internet and maliciously warns you that files on your computer are infected. They direct you to fake sites or urge you to click fake links in order to remedy the problem that never existed in the first place.

# How to Protect Your System

Below are some tips for protecting your computer system and personal/business files against this type of crime, and what to do should you fall victim:

1. Keep your anti-virus and malware software up to date - new ransomware variants appear on a regular basis. Keep your security software up to date to protect against them, if there is an auto-update option with the software then use this option.

2. Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers. As with your anti-virus, if this can be automated then you should always have the most up to date version.

3. Be wary of unexpected emails. Email is one of the main infection methods. Especially if they contain links and/or attachments. If a business email, make sure employees are trained to spot fake emails.

4. Be especially wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.

5. Backing up important data is the single most effective way of combating ransomware infection. Attackers have leverage over their victims by encrypting valuable files and leaving them inaccessible. If backup files are available then the attack fails. Consideration should be given to multi point backups – locally, cloud services and external drives held elsewhere and not connected in any way to the effected systems.

6. Use 2-factor-authentication where available. Most popular website and email systems now allow users to add an additional 2nd layer of security to their accounts. As well as adding a username and password an additional piece of information is required, this can be a fingerprint, message delivered by a text message or a code from an App. Even if an attacker got your username and password they would still not be able to access your account without this additional information.

For further information please visit:

**scotland.police.uk/keep-safe/keep-secure-online/**
**www.nomoreransom.org/en/ransomware-qa.html**
**www.getsafeonline.org/protecting-your-computer/ransomware/**
**www.ncsc.gov.uk/**

POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA