HSBCnet

Malware

Risks to your business:

- Data loss
- Financial loss
- Hardware damage
- Paralysis of business activity

Malicious software is coded with the intention of harming its target. Affecting private and corporate users alike, it can steal information, damage data, hijack website visits and spy on internet activity. Fraudulent redirection of internet banking users is an increasingly frequent form of attack.

What is malware?

Malware can hide inside innocuous-looking software (trojans), or spread between machines without relying on user interaction (worms). It can be custom-designed to evade defences and execute specific tasks.

Once inadvertently installed, malware can carry out many activities unseen. It may spy on website visits, destroy data, or piece together passwords. Increasingly, it's being used by criminals to encrypt important business information until the organisation pays a 'ransom'. Internet banking users might also be redirected to fake sites which record their login data to enable financial theft.

Malware is usually delivered via email 'phishing' or fraudulent links. Malicious apps and USB memory sticks can also compromise smartphones and computers respectively.

Malware can stay hidden for months until activated.

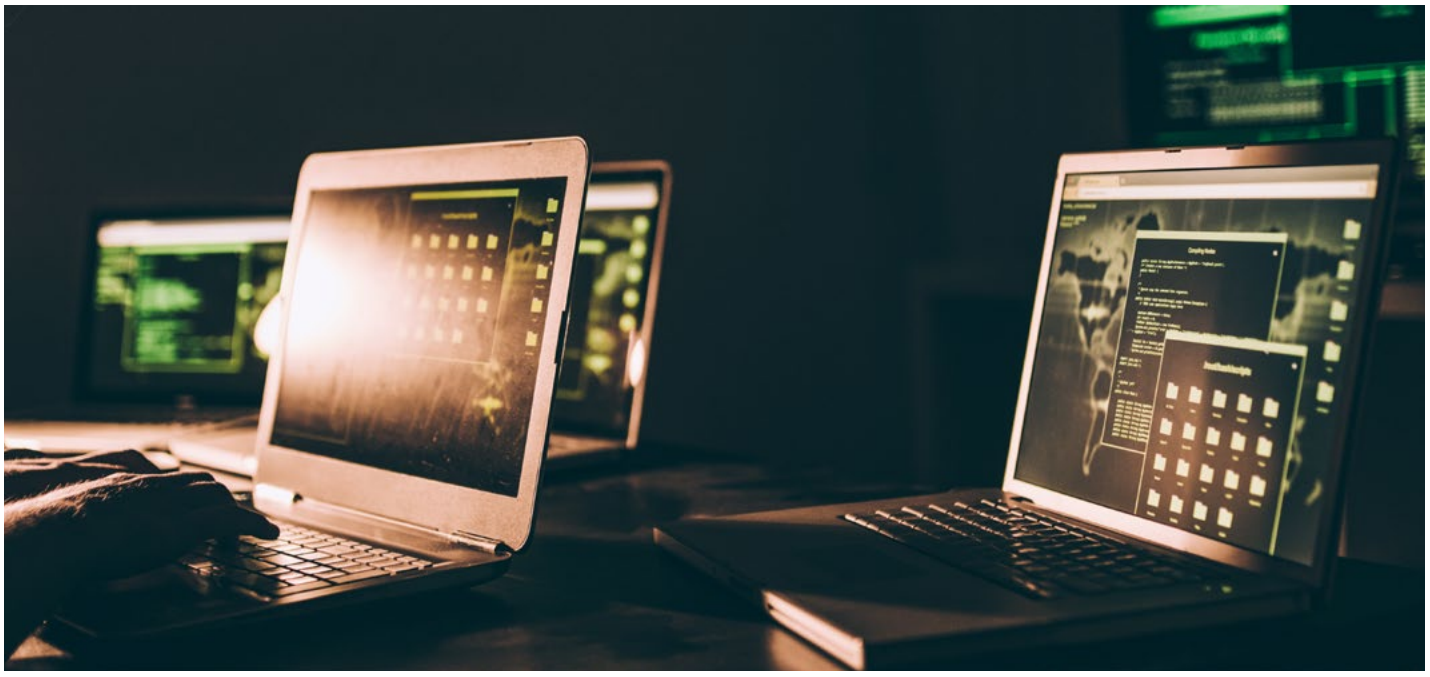
68% **of business security breaches are caused by Viruses, Spyware, and Malware**

Sources: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Types of malware include:

- Spyware
- Trojans
- Ransomware
- Keyloggers

HSBC



The AV-Test Institute registers

390,000

malicious programmes

Every Day

Sources: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

How to keep your business safe:

The scam can appear even more convincing if thieves obtain information about a company's leaders and finance team, for example from the firm's website.

- Put in place strong response, recovery and back-up processes.
- Run up-to-date anti-virus software on all machines in your organisation on a regular, scheduled basis. Frequent anti- virus scans can help minimize the risk of malware attacks.
- Keep your PCs, servers and associated hardware up to date, installing the latest security patches as they become available.
- Make sure that your staff avoid questionable websites, and know not to download free software / apps, run MS Office macros on email attachments, or use USB sticks, from unverified sources.
- Consider application whitelisting (blocking any software not already authorised).
- Use different passwords for different business logins.

If you suspect you have been the victim of fraud, contact your HSBC representative immediately.