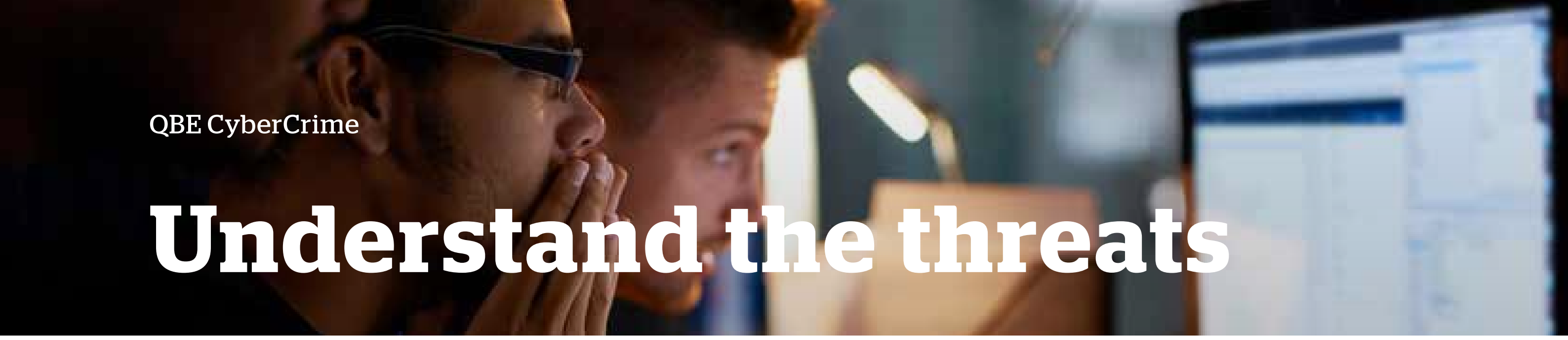

QBE CyberCrime

Understand the threats

Cyber criminals are constantly becoming more sophisticated in the ways that they target businesses, large and small. Here are just some of the threats to be mindful of and some of the IT jargon used.

Adware

Software that can collect personal information, your web browsing history or disrupt your computer with intrusive pop-up adverts.

Backdoor

In many 'normal' computer systems you enter a password and go through the front door. Software developers and companies often build backdoor access into the system for legitimate reasons to allow access to authorised people. Hackers can, however, find these backdoors and use them for their own purposes.

Baiting

A form of social engineering where criminals trick people into clicking onto phoney or malicious websites by offering an incentive, for example 'you have won a prize' or 'download our free report'.

Black Hat Hacker

A 'gun for hire' or a hacker who works for personal / financial gain.

Botnet

Networks of computers controlled by an attacker. By deploying malware to infect random computers a hacker could possibly have control of hundreds of computers without the owners noticing.

Brute Force Attack

An attempt to enter a password-protected system, often by using automated software on a 'trial and error' basis to guess the password and hoping they get lucky.

Bug

An error, flaw or glitch in a software program.

Cracking

Another name for hacking or breaking into a computer system.

Dark Web

We often hear of data being made available on the 'dark web'. This is a collection of websites not listed on search engines like Google. Usually only available to people in the know via specialist networks.

DDOS or DOS

A Distributed Denial of Service, or just Denial of Service is an attempt to cause business interruption to a website or network by flooding it with data requests to the extent that it slows down or brings it to a standstill.

Exploit

A way for a hacker to use a bug in a system to their own advantage, by exploiting the vulnerability.

Firewall

Software / hardware to prevent unauthorised access to a computer system.

Hacker

A person who breaks into a computer system (may be Black Hat or White Hat).

Hacktivist

A hacker motivated by social or political aims, as opposed to financial gain.

Inside Attack

An attack perpetrated by a person with authorised access, for example a disgruntled employees with criminal intent.

Jailbreak

To overcome inbuilt security in a device such as a smartphone or tablet in order to remove restrictions, for example to install an alternative operating system.

Keyboard Logger / Keylogger

A piece of software that records keys pressed on a keyboard, usually in order to capture information such as passwords and credit card numbers.

Malware

Short for 'Malicious Software'. A type of software program designed to damage, disable or infiltrate a computer system.

Phishing

An attempt to gain confidential information, usually by sending an email that looks genuine. The email may contain a link to a phoney website. Phishing emails often purport to come from banks, etc and ask the recipient to verify account details.

Ransomware

A type of malware infection that encrypts the information on a computer or network and effectively locks it down until a ransom fee is paid, usually displaying a threatening on-screen message.

Social Engineering

Any attempt to manipulate or trick people into disclosing confidential information. Examples include a fake email from the company CEO asking to make an urgent payment, a fake phone call from a customer asking for some form of 'help', or a 'baiting' email offering a free report or a link to a free piece of software, etc.

Spear Fishing / Spear Phishing

A more targeted form of phishing, where specific individuals are targeted and the fake email or phone call often appears to come from a trusted source, for example the company CEO.

Spoofing

An attempt to gain unauthorised access or confidential information by impersonating another person. For example, by forging an email address so that the recipient believes it is a genuine email.

Spyware

A type of malware that sits in the background, passing information about computer activity to a third-party.

Trojan Horse

A malicious program that mimics another often more useful program, such as an antivirus program or screensaver. The Trojan Horse can sit in the background on the infected computer, stealing data or downloading spyware.

Virus

A piece of malware that typically relies on other computer users to spread it to other computers, for example by forwarding emails, sharing files or downloading a program.

Whaling

A form of phishing where criminals attempt to 'land a big fish', for example by targeting company CEOs or managing directors with often quite sophisticated scams in the hopes of gaining financial or confidential information.

Worm

A piece of malware that can replicate and propagate its own way through a computer system.

White Hat Hacker

The opposite of a Black Hat. A White Hat will often spot weaknesses and alert companies of potential vulnerability.

Made possible

QBE

A cyber incident can lead to:

- Theft of money, data or goods
- Business interruption
- Reputational damage to your company or brand

What would the cost and the impact be if your business was down for a few days, a week or longer?

It's no longer safe to think "it will never happen to us..."

Get extra peace of mind with QBE CyberCrime Insurance

As business insurance specialists, QBE's new CyberCrime insurance policy has been specially designed to provide SMEs with comprehensive insurance cover and a rapid forensic response to help get you back up and running quickly in the event of an incident.

Ask your broker for a quote for QBE CyberCrime insurance.

QBE for SME
www.QBEeurope.com/sme

Disclaimer

This publication has been produced by QBE Insurance (Europe) Ltd ("QIEL"). QIEL is a company member of the QBE Insurance Group. Readership of this publication does not create an insurer-client, or other business or legal relationship.
This publication provides information about the law to help you to understand and manage risk within your organisation. For full details of the disclaimer surrounding this publication please visit QBEeurope.com/legal/publication-disclaimer.asp

Made possible
QBE

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEeurope.com**

QBE European Operations is a trading name of QBE UK Limited, QBE Underwriting Limited and QBE Europe SA/NV. QBE UK Limited and QBE Underwriting Limited are both authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. QBE Europe SA/NV, VAT BE 0690.537.456, RPM/RPR Brussels, IBAN No. BE53949007944353 and SWIFT/BIC No. HSBCBEBB, is authorised by the National Bank of Belgium under licence number 3093.

156272/MAR19