Risk Solutions

Phone fraud (vishing) Do you know who you're talking to?

Targeting businesses through telephone fraud is on the increase with hackers posing as someone with authority, putting your employees at risk of unwittingly providing confidential information to fraudsters. More than a third of UK businesses suffer an attack or breach at least once a month*, so understanding how to protect your business is vital.

What is vishing?

Vishing is the act of using a phone in an attempt to persuade someone to surrender confidential personal or business information.

Sophisticated fraudsters are targeting organisations to deceive employees into revealing company financial information or transferring money to an account owned by the fraudster. The frauster may pose as someone from a bank or building society, an existing supplier, or someone in your own organisation. They will have a plausible story, such as a bank account number has been changed, or that funds need to be transferred to another bank account. They could also claim to be from your own IT / security personnel or a Microsoft specialist and persuade employees to provide them with access to connect to your computer. This would allow them to place malware or key-logging technology on it.Once the hackers have access, there is a high risk of financial or data loss or operational downtime. Employees can also be tricked to reveal corporate plans or secrets, resulting in the loss of the company's competitive edge.

Tips for employees to manage phone fraud

- Criminals may already have basic information about you or your business in their possession. Do not assume a caller is genuine because they have these details or because they claim to represent a known organisation.
- If you are suspicious or you know it is a cold call, don't be afraid to terminate the call or say no to requests for information.
- If you are requested to provide remote access to your PC, do not give access. Terminate the call and inform a senior person in finance, IT or data security.
- If you are unsure about providing information requested by a caller, tell them you will call them back. Contact someone relevant internally to try to validate the caller and to make sure the information you provide is accurate and allowed to be shared.
- Validate any numbers they provide by checking the website and calling them back on a published number.

* Department for Culture, Media & Sport. Cyber Security Breaches Survey 2017. April 2017

Made possible QBE

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