



Cyber scams

Technology has become a key part of our everyday life whether it is at work or at home. Fraudsters are increasingly using technology as a tool to commit fraud. These types of frauds are known as cyber frauds and are often committed by those with low levels of IT sophistication, but who have access to tools freely available on the web. Cyber fraud is now more prevalent than ever, with instances of data theft and compromised financial systems causing organisations significant losses and reputational damage. Action Fraud reports that 70 per cent of fraud is cyber enabled.

One of the main area of risk is social engineering, where fraudsters deceive and manipulate to convince people to click on email attachments infected with malware, or click on links to a phishing site asking for confidential information. This form of risk relies heavily on a lack of individual awareness, rather than vulnerabilities in software and operating systems. There are a whole host of risks that fall under this umbrella, but those becoming increasingly commonplace are:

Chief executive email scams

Emails arrive from senior members of staff, such as the director of finance or the chief executive, containing requests for urgent payments. The email is accompanied with payment instructions to a specific account used to obtain funds fraudulently. The email is a targeted phishing scam enabled through gaining access to senior members' email accounts or emails sent through a recently registered domain name, which is very similar to the organisation's email address.

Malware

This often arrives in the form of an email which contains a link or an attachment that users are encouraged to access. One example of this form of attack is an email notifying you of a speeding ticket which includes photographic evidence. The aim of these emails is to entice you to click on the link to check the photograph. The link contains malicious software designed to collect information or data from infected devices and pass it on to other devices.

Ransomware

Another form of attack that is worryingly on the increase is ransomware. A click on a link or opening an attachment in an email downloads a virus which sets to work encrypting files. Once the computer is effectively locked down, fraudsters

demand a fee for the return of the files. There is usually a time limit to pay up, after which the ransom increases. One organisation received a phishing email deployed ransomware on its computer system and was requested to pay US\$ 500 (£348) in Bitcoin, the untraceable crypto-currency, for the return of data. Although many of the infected files were restorable from back-up procedures, some services were down for almost a week, leaving staff using pens and paper to do their work.

The people effect

More money than ever is being spent on increased IT defences, but instances of fraud are increasing, why? In part, because of people. Those who use your systems are one of the key risks; whether they are using systems for non-work related activity using their own devices to assist with flexible / remote working or simply undertaking their day to day role and are targeted. Employees often have very low awareness about phishing and social engineering practices that can make them inadvertently help fraudsters. Although regarded as the weak link, employees are also the first line of defence for any organisation.

Preventive measures

Risk management

Cyber risk should be treated in the same way as any other business risk, it is not a matter purely for the IT team, although they clearly play a vital role. The organisation should understand the cyber risks it faces and makes decisions around which risks to avoid, accept, control or transfer. There should be a top level commitment to reduce cyber risks which is communicated throughout the organisation.

Create a culture of awareness.

It's critical that staff understand that data leaks and malicious attacks can occur by just one employee opening a suspicious email, attachment or simply clicking on a link. Deliver a training programme focusing on the cyber risks relevant to job role with real life examples, avoiding jargon and how they should respond. Refresher sessions should be included in the training programme to provide updates on emerging risks and policy/procedural changes.

Basic controls.

Getting the basic controls right: this includes strong password controls, setting user access appropriate for applications, devices and networks and implementing security measures for employees who use their own devices at work. Regular patch management, having a robust firewall and network security control framework as well as malware protection are importance basic controls.

Removable media

Limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organisation's system.

Home and remote working controls.

Enabling staff to work smarter, with greater flexibility and efficiency presents organisations with additional security challenges and risks. Identify the risks associated with this type of working and develop a mobile working policy. Train employees on how to use their mobile devices securely.

Monitoring and review

Risks are not static, regular monitoring is essential to ensure risks are being managed effectively and efficiently. Monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. Monitor systems to identify whether they are being used appropriately in accordance with organisational policies.

If you would like any further advice on cyber fraud please contact your Local Counter Fraud Specialist.

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.