SPECIALIST RISK GROUP

Trade Association Forum
OFFICIAL PARTNER
the association of associations

REMOTE WORKING AND THE RISING RISK OF SOCIAL ENGINEERING

With employees working remotely, cyber-crime a more ominous threat to businesses than ever before.

TAF AND SPECIALIST RISK GROUP SUPPORTING YOUR ASSOCIATION AND YOUR MEMBERS

REMOTE WORKING AND THE RISING RISK OF SOCIAL ENGINEERING

CYBER-SECURITY HAS ALREADY BEEN A SUBJECT OF INCREASING IMPORTANCE IN THE UK FOR YEARS, BUT WITH THE CORONAVIRUS PANDEMIC FORCING MANY ORGANISATIONS TO IMPLEMENT REMOTE WORK, THE THREAT OF CYBER-ATTACKS MUST BE TAKEN EVEN MORE SERIOUSLY.

Cyber-security has already been a subject of increasing importance in the UK for years, but with the coronavirus pandemic forcing many organisations to implement remote work, the threat of cyber-attacks must be taken even more seriously.
One type of cyber-attack that has recently become a more frequent threat is that which uses social engineering.

What Is Social Engineering?

Cyber-criminals conduct social engineering attacks by manipulating people in ways that result in the perpetrator gaining access to property or information that they should not be privy to. Their tactics might include persuasion, impersonation or even intimidation.

Perpetrators may deploy social engineering tactics through a number of different types of cyber-attacks, such as phishing emails, fraudulent online offers or prizes, or telephone scams.

Social Engineering During Lockdown

Most employees working remotely will not have the same level of cyber-security in their homes as an employer would have in its physical workspace. As such, cyber-crime has become an even more ominous threat for organisations of all sizes and across all industries.

The frequency of cyber-attacks has noticeably increased since the beginning of the coronavirus pandemic, and new reports suggest that cyber-criminals are specifically upping their usage of coronavirus-themed attacks. These attacks may come in the form of phishing emails attempting to manipulate recipients into revealing sensitive information by preying on fear or apprehension related to COVID-19.

Given the lack of efficient cyber-security protections as employees work remotely, and the rising threat of social engineering and cyber-attacks related to COVID-19, employers should be especially cautious.

One example of a social engineering attack occurred earlier this year, when a cyber-attack campaign targeted email users around the world with a phishing email. This email claimed to have an attachment from the World Health Organization with advice pertaining to the prevention of COVID-19. However, after opening the attachment and following the email's instructions, malicious software would then be installed on the user's device, providing cyber-criminals with access to confidential information and the ability to install even more malware.

STAYING CYBER SECURE

WITH EMPLOYEES WORKING REMOTELY, THERE ARE FAR MORE POTENTIAL EXPOSURES TO AN ORGANISATION'S NETWORK AND DATA.

Organisations should take the time to assess and address these risks.
Precautionary measures that should be considered include:

1. Provide formal employee training, including guidance regarding specific types of social engineering threats and how to recognise them.
2. Limit employees' ability to access USB ports on company equipment in order to reduce the chance of a virus or malware infecting the device.
3. Implement a virtual private network (VPN) in order to mask organisational data, such as web traffic.
4. Use layers of protection, such as multi-factor authentication. In the event that a password is compromised, having additional layers that cyber-criminals must penetrate reduces an organisation's risk.
5. Review user accounts and their level of access to sensitive information. Limiting accounts access to information relevant to employees' duties will help limit potential damage in the event that any accounts are compromised.
6. Invest in cyber insurance which provides cover to respond to a cyber-breach or attack and ensures your business is not liable for the costs and efforts associated with dealing with the consequences of the incident.

HOW WE CAN HELP

FOR MORE INFORMATION ON SOCIAL ENGINEERING AND CYBER-SECURITY, CONTACT OUR CYBER EXPERT LAURENCE OWENS:

020 7977 4800
srisenquiries@specialistrisk.com
srinsurancesolutions.co.uk

Provided by Specialist Risk Group