HSB

A Munich Re company

Technical bulletin

Cyber security

How to treat three common cyber tricks

Under the cover of the dark web, cyber criminals are refining their sinister methods; and they're only becoming more sneaky and destructive.

Here are three of their most common tricks and how you can avoid getting fooled.

1 You receive a phone call advising that your computer is infected

Here's one of the most common schemes: You receive a call from someone disguised as an IT technician who claims your computer has a virus, and for £150 they can fix your problem by accessing your machine remotely.

You provide your payment information and log-in credentials, and it appears that the technician is 'fixing' your computer. In fact, they are either doing absolutely nothing, or downloading malware to transmit your personal and financial information. Scary, right?

How do you prevent this menacing scam?

- Document the phone number of the caller and their name
- Hang up
- Block their number from calling again
- Report the matter to:
  - England and Wales: Action Fraud
  - Scotland: Police Scotland

No reputable computer security company or software firm calls to inform anyone that they have a computer virus. Normally, your firewall will prompt a message prior to accessing a bad file or site, and your anti-virus software will scan and fix your files automatically. Check with your Internet Service Provider, because you may already be receiving these services at no additional cost.

2 You receive a shocking email

An email arrives into your in-box with a subject line that says, "Your payment of £3,100 to PayPal has been approved", or "I am NOT paying this invoice".

You can't resist the urge to open it. It might seem like you're due to receive a lot of money, or being accused of something you didn't do.

Emails with subject lines like these are remarkably successful in luring their victims into opening them. The real danger lies in the links. Clicking on these could open the door to malicious software, with ransomware being the usual suspect.

How to prevent this sinister scam?

- Beware of signs that an email is malicious or fraudulent
- Alert your IT security department immediately so other employees can be warned and protected. If you are a smaller business, run a virus scan and monitor your customer, company and financial information
- Delete the email

3 You are tricked into transferring funds by an imposter

A business email compromise (BEC) can take many forms, but the most prevalent and costly iterations combine insider information (obtained by hacking or social engineering) with emails.

The BEC scam usually starts off with an email that makes a pressing demand. It appears to come from an executive or trusted vendor who is unavailable to confirm the demand.

The sender demands that you transfer funds immediately to facilitate a deal or to pay an invoice. The receiver may be deceived by the sender's inside information, such as details of a pending deal or specific relationship.

How to prevent this nefarious scam

- Watch for emails that demand you make a funds transfer, change vendor information, or supply personal or financial information
- Before taking action, confirm the request verbally; either by phone to a known number or in person
- If you received the email via your work email account, alert your IT security department and the appropriate internal contact immediately so that preventive actions can be taken; such as blocking the scammers and raising your colleagues' awareness

Awareness of these cyber tricks is your best defence. Whether you're home, at work or out using your mobile device, always be on the lookout for cyber threats lurking in unexpected places.

For more helpful tips, visit The National Cyber Security Centre's website.

Reproduced with kind permission from The Hartford Steam Boiler Inspection and Insurance Company. For more insights, visit their Equipment Connection blog.

HSB
A Munich Re company

www.hsbeil.com HSBEI-2064-0622-2 Picture credits: Getty Images