BUSINESS EMAIL COMPROMISE

REVAK
SECURITY AND INTELLIGENCE SERVICES

Business Email Compromise is when an unauthorised user accesses your email account, usually to steal money, obtain business information or cause disruption. They often monitor your emails for a while before acting, to identify key contacts or financial habits. The main tactics used to compromise your account are:

MALWARE

Meaning 'malicious software', malware includes viruses and spyware that's often included with a download (such as a screensaver or toolbar) from an untrustworthy source. It can steal login information, log keystrokes or monitor your online activity, and can lead to serious problems like identity crime and fraud.

ATTACKING WEBSITES

Criminals break into websites and steal account information. This can be checked to see whether passwords have been re-used on other websites.

PHISHING

Criminals can often send emails or text messages appearing to be from official sources, tricking people into sending their account data.

IF YOU THINK YOUR EMAIL HAS BEEN COMPROMISED, IT'S ESSENTIAL TO REMEDIATE IT STRAIGHT AWAY.

- Scan all your devices for malware and viruses, deleting suspicious software.
- Ensure your devices and software are updated to the latest operating system and version
- Change your email passwords and any other internet accounts with the same password
- Inform your contacts to be cautious of any emails received from you
- Check your settings to ensure there are no 'rules' forwarding your emails elsewhere
- Change your security questions and answers
- Check your sent folder for any suspicious emails you haven't sent, and contact the recipient
- Have backups of your company information stored separately from your primary device

HOW CAN I BE SAFER?

If you suspect malware, stop doing things that require passwords or personal info, such as online shopping or banking. Use a different computer to change your passwords. Protecting yourself requires implementing a number of security controls, such as:

- Ensure all devices automatically install security updates
- Turn 'autoplay' off
- Turn on Multi-Factor Authentication for internet accounts
- Never share passwords with coworkers, friends or family
- Ensure a website has a HTTPS address before sharing personal information with it
- Use a password manager to generate and store passwords, not your browser.
- Be wary of urgent emails. Criminals may try and rush you into a mistake
- Stay vigilant, follow these tips, and don't allow complacency to creep in

AFTER IDENTIFYING AND REMEDIATING A BREACH, YOU'RE LIKELY TO BE TARGETED AGAIN

Repeat victimisation is common as criminals often return to the businesses or individuals they have successfully compromised. It is essential you follow the below tips:

1. Check the sender of emails received before reading them as display names and email addresses can appear to be from anyone
2. Don't click any links or open documents from any emails from unknown sources
3. Hover over links to ensure the destination is what you expected
4. Verify any request to change or provide personal information with the sender by telephone, even familiar contacts
5. Regularly check bank accounts and immediately inform the bank of any suspicious transactions
6. Regularly check 'sent' folders to identify suspicious emails that may have been sent from your account

info@revak.uk www.revak.uk @RevakUK

afi Association of Fencing Industries