Cyber risks

10 steps for avoiding a business email compromise/fraudulent transfer event

What is business email compromise?

According to the FBI, a business email compromise (BEC) is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

What you can do

Beware of phishing

Be on the lookout for emails with urgent, fear-inducing subject lines, or updates from scammers posing as someone from your company. Hover over the email sender's address with your mouse to ensure it's from your company, and hover over links to preview their destination. If you're not sure about it, don't click it.

And vishing (voice phishing)

Never provide your login information, financial account, or allow access to your devices to someone over the phone, unless you've confirmed the request is from a trusted source.

Keep software up to date

Putting off installing updates to your computer and phone software can expose you to cyber attacks. Install updates as soon as possible.

Use multi-factor authentication

Multi-factor authentication is an added layer of security users are required to acknowledge a phone call, text message, or an app notification on their smartphone after correctly entering their password. Only after this second authentication factor has been satisfied can a user sign in.

Passwords

Use complex, hard-to-guess passwords that contain random words, a combination of capital and small letters, numbers and symbols. Change passwords frequently or use a password manager and multi-factor authentication.

What your organization can do

Train employees

Make sure employees understand your policies for computer access and using their own devices. Train employees in good cyber hygiene — how to spot phishing emails, use of complex passwords, and how to report and respond to a suspected business email compromise.

Firewalls

Make sure your IT team employs firewalls for your internet access to protect your team from viruses, ransomware, and other cyber attacks.

Admin rights

Limit access to servers and software to employees who require it for their job. Implement a policy requiring multiple internal parties to confirm authorization (such as a call back) before making payments (including wire and ACH transfers) in excess of large amounts, such as $10,000.

Secure Wi-Fi networks

Your Wi-Fi should be secured with a password. When off-site, only log in to secure Wi-Fi networks that require a password. Do not set your device to log in automatically to networks that are not secured.

If you think you've been hacked, act

If you think you've been victim to a cyber crime, immediately call the appropriate internal or external resource and notify your agent or insurer if you have a claim.

HSB™
A Munich Re company

2023-131 (Rev. 5/23)