HSB

A Munich Re company

Cyber risks

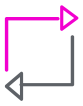
10 tips for cyber security

Risk management

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 log-in 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.

Back up data
Be sure to back up your data, so you can access it outside of your system, in case you are hit by a cyber attack.

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 organisation can do

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

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.

Secure Wi-Fi networks
Your Wi-Fi should be secured with a password. When off site, only log into 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 broker, intermediary or insurer if you have a claim.

HSB Engineering Insurance Limited, registered in England and Wales: 02396114, New London House, 6 London Street, London EC3R 7LP. Registered as a branch in Ireland: 906020, 28 Windsor Place, Lower Pembroke Street, Dublin 2. HSB Engineering Insurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom and is regulated by the Central Bank of Ireland for conduct of business rules.

www.hsbeil.com HSBEI-2193-0320 Picture credits: Getty Images