

# 10 tips for cyber security

## 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.



**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 organization 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 WiFi networks**  
Your wifi should be secured with a password. When off site, only login to secure wifi networks that require a password. Do not set your device to login 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.