Staying Cyber Safe

A working from home guide for business owners and their employees

With record numbers of Australian businesses and employees moving to remote working during the COVID-19 pandemic lockdowns, being alert to cyber risk is of increased importance.

Gallagher's Cyber Risk team understands the added disruption and anxiety that results from a successful cyber-attack and the impact of the subsequent loss of sensitive data. This guide is designed to provide useful information about how to protect the company's data, network resources and sensitive information while working remotely.

Understanding common cyber-attacks and how to avoid them

Remember that technical defences, while good, cannot fully protect you or your organisation. Attackers know that employees can be targeted using unfamiliar cyber techniques, **however you and your actions remain the best defence against these attacks.**

To help minimise risk to your company's network and data, we suggest employees take these actions while working remotely.

Phishing, watering-hole, and other 'social engineering' attacks

What this is and how it happens

Typically phishing (pronounced 'fishing') is an email with a tempting 'lure' – such as a message about an urgent issue or a promise of sharing critical information – designed to trick users into taking a detrimental action like clicking a link or opening an attachment. 'Watering-hole' tactics are actions that take users to a site (URL) that is configured with malicious code, which then enables the security of data and information to be compromised.

Stay cyber safe: tips to avoid cyber-attacks

- Do not click on untrusted links or open attachments to emails from unknown parties. These links and attachments can look sophisticated and mirror the branding and appearance of legitimate sources. If unsure, contact the sender by telephone, via a trusted email address, or contact your IT helpdesk and ask for assistance.
- Beware of emails and other messages that relate to breaking news, surprising information, or other urgent messages – particularly those related to COVID-19 – asking you to 'act now'. Be cautious of both the email sender and email address and use appropriate caution with emails from unfamiliar names, sender addresses with enticing email subject lines.
- Visit only trusted websites for updates on the COVID-19 pandemic, and other business/market related information relevant to normal business operations. Beware of websites advertised in social media posts or sites attracting attention through the use of urgent or inflammatory messages.
- You may also be asked to provide information via unexpected multifactor authentication requests. **If you receive a request to approve a connection you did not ask for**, do not approve the request and report the incident in the usual way to your IT helpdesk or support team.
- Limit unnecessary or recreational browsing using company equipment or assets (i.e. laptops, mobile devices). Legitimate websites and/or information sources may become compromised and used to distribute malicious software (or 'malware'). Avoid allowing family members to use company-owned equipment for personal purposes, which can expose the system to unexpected browsing activity and cyber related issues.

Controlling data sprawl and loss

What this is and how it happens

Remote working commonly leads to data sprawl - essentially, data that is placed outside the company's standard IT/cyber defences and information security practices. Employees working from remote locations are more likely to take actions that expose the business to risks that would normally be less evident in a standard office or business working environment.

For example, an employee trying to print or share a sensitive file and then sending the file to a personal email address, exposes the data (information contained within) to potential loss. Alternatively, an employee may transfer files to an insecure portable storage device, such as a USB stick, that is then either lost or misplaced.

Another aspect to the data movement and sharing risk is if an employee elects to transfer or share files through an unapproved cloud-storage account or other non-approved file-sharing platforms, thereby exposing the data to misuse or misappropriation.

Stay cyber safe: tips to avoid cyber-attacks

Use only company approved solutions to transfer data:

- For internal and external collaboration, conferencing and file sharing - only use company approved file-sharing and collaboration tools to transfer information and data.
- Do not use unauthorised file-sharing sites (e.g. Box, YouSendIt, Dropbox).
- Do not email data to personal email accounts or transfer data to unapproved portable storage devices (e.g. USB memory stick).
- Do not email unencrypted, commercially sensitive data to external parties. If you need to send an individually encrypted file, secure it with a strong password, and do not share the password by email. Better still, use a company approved transfer solution.

Using secure networks and remote access security best practice

What this is and how the cyber risk arises

With larger volumes of remote access usage across the company, the risk of a cyber attacker gaining access to the network rises significantly, despite processes designed to secure your network from unauthorised remote access.

Attackers may try to collect user credentials for email, virtual private network (VPN), and other remote access systems through phishing emails designed to harvest users' credentials. They may also try to bypass multi-factor authentication controls by tricking users into approving an authorisation request.

Connections to insecure networks (whether at home or in public locations) can also expose systems and data to attack. This can occur, for example, when using home routers with insecure settings or open public networks.

Stay cyber safe: tips to protecting data on remote networks

- Use secure, known networks. Use a company-provided VPN wherever possible – the VPN offers an added layer of protection for possible insecure networks.
- If either you or a family member has the technical ability to do so, ensure your home Wi-Fi router is protected with the WPA2 or WPA3 encryption setting; ensure your router/modem and internet service provider (ISP) portal are configured with a strong, unique password; and ensure software for all routers and modems is regularly updated.