How to prevent major cyberthreats facing remote workers

Remote work has transformed the way businesses operate, but it has also introduced unique cybersecurity challenges. We've compiled a comprehensive list of the major cyberthreats facing remote workers and those managing a remote workforce, along with actionable tips to mitigate these risks.

THREAT
Phishing attacks

Cybercriminals use fraudulent emails or messages to trick employees into revealing sensitive information or clicking on malicious links.

PREVENT

- Conduct regular phishing awareness training for employees.
- Use email filtering tools to block suspicious emails.
- Implement multi-factor authentication (MFA) to add another layer of security.

THREAT
Weak passwords

Employees using simple or reused passwords make it easier for cybercriminals to access accounts.

PREVENT

- Enforce strong password policies and periodic password changes.
- Provide access to a company-approved password manager.
- Implement multi-factor authorization (MFA) for all critical accounts.

THREAT
Unsecured Wi-Fi networks

Public or unsecured networks expose sensitive company data to interception by hackers.

PREVENT

- Require employees to use a secure VPN when connecting to company systems.
- Educate staff on the risks of public Wi-Fi and encourage using personal hotspots.
- Disable file sharing and Wi-Fi direct on devices to prevent unauthorized file access.

THREAT
Unpatched software and systems

Outdated software may contain vulnerabilities attackers can exploit.

PREVENT

- Set up automatic updates for operating systems and applications.
- Regularly audit company devices to ensure they are updated.
- Monitor using endpoint detection and response (EDR) tools.

THREAT
Insecure personal devices

Employees working on personal devices without proper security measures can expose company data.

PREVENT
- Provide company-managed devices preloaded with security tools.
- Require endpoint protection software on personal devices used for work.
- Implement policies for separating personal and professional activities.

THREAT
Ransomware attacks

Cybercriminals use ransomware to encrypt company data and demand decryption payments.

PREVENT
- Maintain regular, encrypted backups of critical data.
- Educate employees about suspicious links or downloads.
- Use advanced anti-malware software to detect ransomware.

THREAT
Lack of secure collaboration tools

Using unapproved or unsecured communication and file-sharing tools can lead to data leaks.

PREVENT
- Provide secure collaboration tools (e.g., Microsoft Teams, Slack or Google Workspace).
- Regularly audit the tools employees use and prohibit unauthorized applications.
- Encrypt files before sharing.

THREAT
Shadow IT

Employees using unauthorized apps or services can bypass IT security controls, creating vulnerabilities.

PREVENT
- Create an approved list of software and tools for work use.
- Provide employees with alternatives to commonly used tools to reduce the temptation to use unapproved ones.
- Monitor network traffic to identify shadow IT usage.

THREAT
Social engineering attacks

Cybercriminals manipulate employees into divulging confidential information through personal interaction.

PREVENT

- Conduct role-specific training on recognizing social engineering tactics.
- Encourage employees to verify requests for sensitive information through trusted channels.
- Promote a culture of reporting suspicious activity.

THREAT
Data leakage from remote workspaces

Sensitive data might be exposed if employees work in shared or public spaces.

PREVENT

- Encourage the use of privacy screens on laptops.
- Advise employees to avoid discussing sensitive information in public areas.
- Limit offline access to sensitive files.

THREAT
Weak home network security

Poorly secured home networks can be a gateway for attackers.

PREVENT

- Educate employees on securing their home routers (e.g., change default passwords and enable WPA3 encryption).
- Provide a checklist for securing IoT devices on home networks.
- Offer IT support to audit and secure home setups if possible.

THREAT
Lack of incident response plans for remote workers

Delays in responding to incidents can amplify damage during a cyberattack.

PREVENT

- Develop a remote-friendly incident response plan.
- Train employees on how to report and respond to incidents quickly.
- Regularly test response plans through simulated drills.

Cybersecurity for remote and hybrid workers requires a multi-layered approach combining technology, policies and employee awareness.

By addressing these threats proactively, businesses reduce risk and protect their operations from costly breaches.

Need help creating a robust remote work security plan?
Contact us today to safeguard your business and confidently empower your remote workforce.

IT & T PTY LTD (ITT) (TA-0-8204-8462-6393)
Email: info@itt.com.au
Phone: +611300482638
https://www.itt.com.au