Security tips for organizations with remote workers

March 2024 **ITSAP.10.016**

Remote work introduces some challenges when trying to balance functionality with security. When working remotely, your employees need to access the same internal services, applications, and information that they would have access to in the office. However, your organization also needs to protect your systems and information, as remote work introduces new vulnerabilities. You need to implement additional security precautions to prevent threat actors from taking advantage of those vulnerabilities.

Understand the threats to remote workers

Remote work can increase the likelihood of compromises to your organization's sensitive information. Threat actors use different methods to target remote workers:

- **Physical access to a device:** If employees leave devices unattended in public, a threat actor can tamper with them or steal them
- **Phishing:** A threat actor emails, texts, or calls victims and poses as a legitimate organization requesting sensitive information, such as passwords, or credit card numbers
- **Social engineering:** A threat actor may gather information about your organization or an employee to craft a targeted phishing message
    - Any information that is posted online can be used, whether it is on a corporate website or personal social media
- **Ransomware**: A threat actor uses malware to access a device and the data on it then denies access until a sum of money is paid
- **Wireless hijacking:** A threat actor spoofs a Wi-Fi network by creating a network that uses the same name as a legitimate one, for example, a coffee shop's public Wi-Fi network
- **Eavesdropping:** A threat actor listens to Wi-Fi traffic and records online activities and account passwords
- **Traffic manipulation**: If a mobile device is infected with malicious code, a threat actor can insert their own traffic to influence data and obtain access to your organization's network

Manage mobile devices

If possible, your employees should use corporately owned devices when working remotely. Remind employees to follow your organization's policies and use devices appropriately

If employees are using personal devices for work, keep the following risks in mind:

Lack of security updates: Personal devices may not be updated or patched regularly, leaving vulnerabilities unaddressed

Weak password practices: Personal devices may not be protected with a PIN or password, and even if they are, easily guessed PINs or passwords may be used

Loss of control over information: If used for work purposes, personal devices may hold sensitive business information that your organization can't manage appropriately

Remind employees to follow organizational policies when using personal devices, and communicate best practices for securing devices. For example ensure employees are enabling multi-factor authentication (MFA), using anti-virus software and never leaving devices unattended in public. To learn more, see Secure your accounts and devices with multi-factor authentication (ITSAP.30.030).

Prepare your employees

If an employee has never worked remotely before, the transition can be surprisingly difficult. Set your employees up for success and clearly communicate the measures that they need to take to contribute to your organization's cyber security.

- Have policies and procedures in place that outline, for example, the acceptable use of corporate devices and the management of corporate information
- Ensure your employees know who to contact, especially if they experience security issues, or their devices are lost or stolen

Train your employees on cyber security issues and best practices, such as:

- spotting phishing attempts
- creating strong passphrases and passwords
- using secure Wi-Fi networks

AWARENESS SERIES

Cat no. D97-1/10-016-2024E-PDF
ISBN 978-0-660-70530-9

Use security tools

There are security tools that your organization can use to add additional layers of protection for your networks, systems, and devices.

Security tools can reduce the risks to your organization, but keep in mind that no tool is perfect. You should never rely on a tool alone. Be sure to implement other security controls as well. The security tools below are just some examples of ways that you can reduce the risks of malicious intrusions caused by malware or other cyber attacks.

Virtual private network

A virtual private network (VPN) is a secure, encrypted tunnel through which information is sent. You can use a VPN to establish a secure connection that uses authentication and protects data. Using a VPN ensures that your organization's communications stay private through an untrusted network. Let your employees know that they must use a VPN to connect to work servers.

Firewalls

A firewall is a security barrier placed between 2 networks. It controls the amount and the types of traffic that can pass between the networks. A firewall adds to your security by monitoring all incoming and outgoing traffic and filtering out known-bad traffic.

Anti-virus software

You should use anti-virus software and ensure that this software is updated regularly. Anti-virus software defends devices against malware by scanning files and your system.

Application allow listing

Application allow listing is a technique used to control which applications can run on corporate devices. Your organization can create an allow list that defines all approved applications, preventing users from running and installing unauthorized software on corporate devices.

Replace end-of-life devices

Devices that have reached end-of-life (EOL) pose a security risk to your organization. EOL means that the vendor stops marketing, selling, and providing support and updates to the device. When you use devices that are not updated to the latest firmware, you can open yourself up to cyber attacks. Firmware is the software that is installed and updated by the manufacturer and contains important security measures. You can check whether your router is EOL by looking at the vendors end-of-life product list or accessing the routers records in its system logs.

Protect devices

With employees working from home or public locations, you should take the following measures to protect devices. Encourage employees to take the same measures on their personal devices as well.

- **Use multi-factor authentication:** To add an additional layer of protection, require two or more authentication factors to unlock devices, such as a PIN and a fingerprint
- **Use password-activated screensavers:** When a user is inactive after a defined period, their device locks
- **Turn off Bluetooth or Wi-Fi when not in use:** Turning off Bluetooth and Wi-Fi prevents threat actors from attempting to connect to and access devices
- **Update and patch.** Set up devices to run automatic updates for operating software, primary applications, and security software. Confirm hardware is still supported.

Protect information

Your organization is responsible for protecting the sensitive information that it collects and uses. Keep in mind that sensitive information is a high-value target for threat actors.

- **Back up information:** Information should be backed up regularly and backups should be stored securely
- **Encrypt information:** Use encryption to protect the confidentiality of sensitive information. For example, you should only allow users to access HTTPS-supported websites on corporate devices
- **Apply the principle of least privilege:** Ensure that employees only have access to the information that they need to do their jobs. Controlling access can prevent unauthorized access to data and data breaches

Learn more

The tips above are a great place to start. To learn more, read through some of our related publications:

- Protect your organization from malware (ITSAP.00.057)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Virtual private networks (ITSAP.80.101)
- Social engineering (ITSAP.00.166)
- Ransomware: How to prevent and recover (ITSAP.00.099)
- Routers cyber security best practices (ITSAP.80.019)
- Obsolete products (ITSAP.00.095)