CROWDSTRIKE
business resilience

Best Practices

Security Awareness: Remote Worker

Many organizations now support remote work environments, bringing new challenges for security. Understanding and implementing effective security practices is important to safeguard your organization and its people. By following best practices, remote workers can minimize risks and maintain a secure working environment.

Do's and Don'ts

Working remotely means you must be even more vigilant to protect your organization's information. Follow these key do's and don'ts to help you maintain strong security habits and avoid common attacks:

- Don't click on links or attachments from unknown sources
- Don't provide sensitive information to unauthorized personnel
- Never provide PII outside of your organization
- Be wary if asked to provide account information
- Be alert if you notice grammar and misspelling on a request
- Verify social media messages are from a legitimate source
- Always keep control of your equipment and stored data

WiFi and Device Security

Securing your WiFi network is very important in preventing cyberattacks, especially for remote workers. An unsecured WiFi network can expose important data and can leave the company vulnerable to unauthorized access. This list can help you understand how to avoid such threats:

- Log into the recommended VPN before accessing your organization's network
- Check for a preferred HTTPS connection when accessing a website
- Secure your devices from being accessed by unauthorized people (including your family and friends)
- Make sure you are in a private setting for any meetings or calls where sensitive information might be discussed
- If you're not on your home network and are using a public WiFi, limit your work to things that are not sensitive

Reporting

When remote, you should follow the same reporting guidelines as when you are working in an office environment.

Get more resources from CrowdStrike for creating your own Security Awareness Program →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.