

☰ Shifting operations to a work from home (WFH) model introduces new cybersecurity considerations to your organization. Use this checklist to get ahead—and stay ahead—of new risks.

- Perform a cybersecurity health checkup** during and after the shift to WFH. Review all cybersecurity controls to identify gaps, prioritize, and remediate accordingly.
- Update your Technology & Data Use Policy** to include remote workforce considerations like non-company owned Wi-Fi, VPN usage, USB and connected drives, and Bring Your Own Device (BYOD).
- Update your Incident Response Plan** to include common and key WFH scenarios that may impact your organization, including lost or stolen devices.
- Send regular awareness training videos** to employees, depicting important cybersecurity topics for a remote workforce, such as Wi-Fi usage and actively protecting company devices.
- Hold group classroom training sessions** via remote webinar with employees on best practices to help protect the company. Include a short quiz to gauge learning.
- Share engaging digital infographic posters** via chat, Intranet and communication tools to keep cybersecurity terms and best practices top of mind for all employees.
- Get regular cybersecurity threat alerts** that feature emerging cybersecurity topics, attacks, and vulnerabilities—including those related to remote workforce.
- Run vulnerability scans on networks** (internally and externally) any time you make configuration changes to firewalls and other devices, including VPN, to quickly identify critical vulnerabilities to patch.
- Scan the Dark Web for stolen passwords** for all employees. If any are found, have employees change passwords immediately on all systems, devices, and applications.
- Activate ongoing phishing tests** on employees simulating how cyberattackers use fear, uncertainty, and doubt. Employees should confirm requests and verify links or attachments before opening
- Complete ethical hacking on your networks** after reconfiguring systems to identify weaknesses attackers could exploit. Remediate gaps to strengthen boundaries.

Defendify makes cybersecurity manageable and easy to understand through a single pane of glass. How can we help you check the box? For more information, please visit www.defendify.io

