CHECKLIST

REMOTE WORK CYBERSECURITY FOR IT

If you are new to work-from-home cybersecurity or just want to ensure you are meeting technical best practices, here's a quick checklist to help ensure the safety of your organization's network:

- ✓ **Set up Multi-Factor Authentication (MFA) whenever and wherever possible.** This is especially important for employees that have roles in management, finance, and IT since they are often targeted in scams.
- ✓ **Make sure employees know NOT TO RE-USE PASSWORDS.** This is one of the top ways that organizations get hacked.
- ✓ **Give employees access to a password manager,** to help them select strong, unique passwords.
- ✓ **Require passwords to be long,** ideally 16 characters or more, whenever possible.
- ✓ **Require a strong PIN or passcode** for all remote work desktops, laptops and mobile devices.
- ✓ **Use a Virtual Private Network (VPN)** to protect your internal network instead of allowing direct login.Make sure your VPN is properly hardened. Key tips include:
  - Implement protections against brute-force password guessing
  - Make sure your VPN software is up-to-date [see VPN vulnerability]
  - Use certificate-based authentication, in addition to a password, to reduce the risk of unauthorized login and login from a non-approved device.
- ✓ **Never open Remote Desktop Protocol (RDP) to the public-facing internet.** If you must to do this for emergency reasons, there are steps you can take to secure an open RDP interface, such as IP-based whitelisting, key-based authentication and more. Contact LMG Security for advice.
- ✓ **Implement automated screen locking** for any devices that are under your control which may contain sensitive data.
- ✓ **Train employees to lock their screens** when they are away from their devices.
- ✓ **Consider purchasing privacy screens, laptop locks or other low-cost physical security tools** for employees that work from home.
- ✓ **Ensure that mobile devices and remote workstations are routinely patched and updated**, just like your internal systems. Many VPNs can be configured to scan remote systems and ensure that they meet minimum security standards before connecting.
- ✓ **Deploy antivirus on all remote systems** and ensure that they are kept up-to-date. If you have decided to support BYOD, consider purchasing antivirus licenses for your employees' personal devices that are used for work.

- **Encrypt all laptops, desktop computers and mobile devices** that are used in remote locations.

- **Keep track of company-owned devices that you deploy for remote use!** If employees have already taken equipment home, you can conduct a survey to gather information about what equipment people have taken.

- **Secure your cloud software that you roll out.** Many popular products such as Office365 include built-in security tools and helpful security checklists.

- **Use a mobile device management (MDM) solution** for laptops and mobile devices so that you can remotely manage and/or wipe a device if necessary.

- **Take advantage of cloud MDM features** designed to reduce the risk associated with mobile devices. Popular cloud software suites such as G-Suite and Office365 enable you to manage device access and even remotely wipe sensitive data from the employee's device.

- **Restrict employees' ability to download documents from the cloud,** whenever possible.

- **Enable logging and monitoring capabilities** on any newly-deployed laptops, mobile devices, cloud resources, VPN, etc. Make sure to collect both failed and successful logins, as well as activity and access logs.

- **Secure your videoconference software.** Make sure you that you understand security best practices and communicate important tips to users clearly and regularly.

- **Ensure employees only use approved cloud services.** Many employees may be tempted to use personal file sharing sites such as DropBox or Google Drive to simplify remote work without realizing that they can cause cybersecurity issues.

- **Consider deploying data-loss prevention (DLP) software** for your email and other resources, to reduce the risk that employees will send sensitive data to personal email addresses, or otherwise circumvent security measures.

- **Make sure that users have an easy way to report suspicious activity** or a lost/stolen device to the appropriate contact.

With awareness and education, security can be maintained from wherever work is getting done. Stay healthy and be well!

*If you need help defining work from home cybersecurity policies and procedures or testing to check for gaps in your newly expanded network, **contact us**, we can help.*

LMG™
SECURITY

145 W FRONT STREET
MISSOULA, MONTANA 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support.
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855 | E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com