

REMOTE WORK CYBERSECURITY FOR EMPLOYEES



As you work from home, remember good cybersecurity hygiene keeps you and your organization safe! Follow these best practices:

- ✔ **Know your organization's remote work policies and follow them.**
- ✔ **Watch out for phishing emails and phone scams.**
- ✔ **Define your physical workspace and communicate boundaries.**
- ✔ **Do not share company computers or mobile devices with family members or roommates.**
- ✔ **Set a strong password or PIN** for all devices.
- ✔ **Use multi-factor authentication (MFA)** whenever possible.
- ✔ **Do not re-use passwords** for multiple accounts.
- ✔ **Use a password manager if one is available to you.** If you are using a cloud-based password manager, make sure to use MFA to protect your account.
- ✔ **Use anti-virus software** and keep it up-to-date.
- ✔ **Keep your work and personal accounts separate whenever possible.** Do not copy sensitive work data to your personal computers or personal mobile devices unless you have received authorization in writing from a manager.
- ✔ **Do not upload sensitive data** to the cloud or personal email unless you have received authorization in writing from a manager.
- ✔ **Secure your home wireless network.** Set a strong password (not the default) and use WPA2.
- ✔ **Use locks when possible,** such as lockable doors and storage spaces.
- ✔ **Maintain a clean desk.** Putting sensitive information out of sight helps to protect it from accidentally being viewed.
- ✔ **If you have a privacy screen for your computer,** use it to help prevent unauthorized access.
- ✔ **Lock your screen whenever** you step away from your computer, particularly if you are in a shared living space.
- ✔ **Set an automated screen lock on all devices** that contain sensitive data, so that if you get up from your desk, it locks the screen after a predetermined amount of time (ie 15 minutes).
- ✔ **Do not write down passwords** and store them in an unlocked location.
- ✔ **Follow your organization's secure disposal policies.** Do not dispose of sensitive data in normal trash.
- ✔ **Keep track of what company devices/furniture you have at home.** Provide this information to your company proactively, if possible.
- ✔ **Immediately report anything suspicious,** including unauthorized access or suspicious activity, to an appropriate contact at your organization.



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



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