Oaccess one

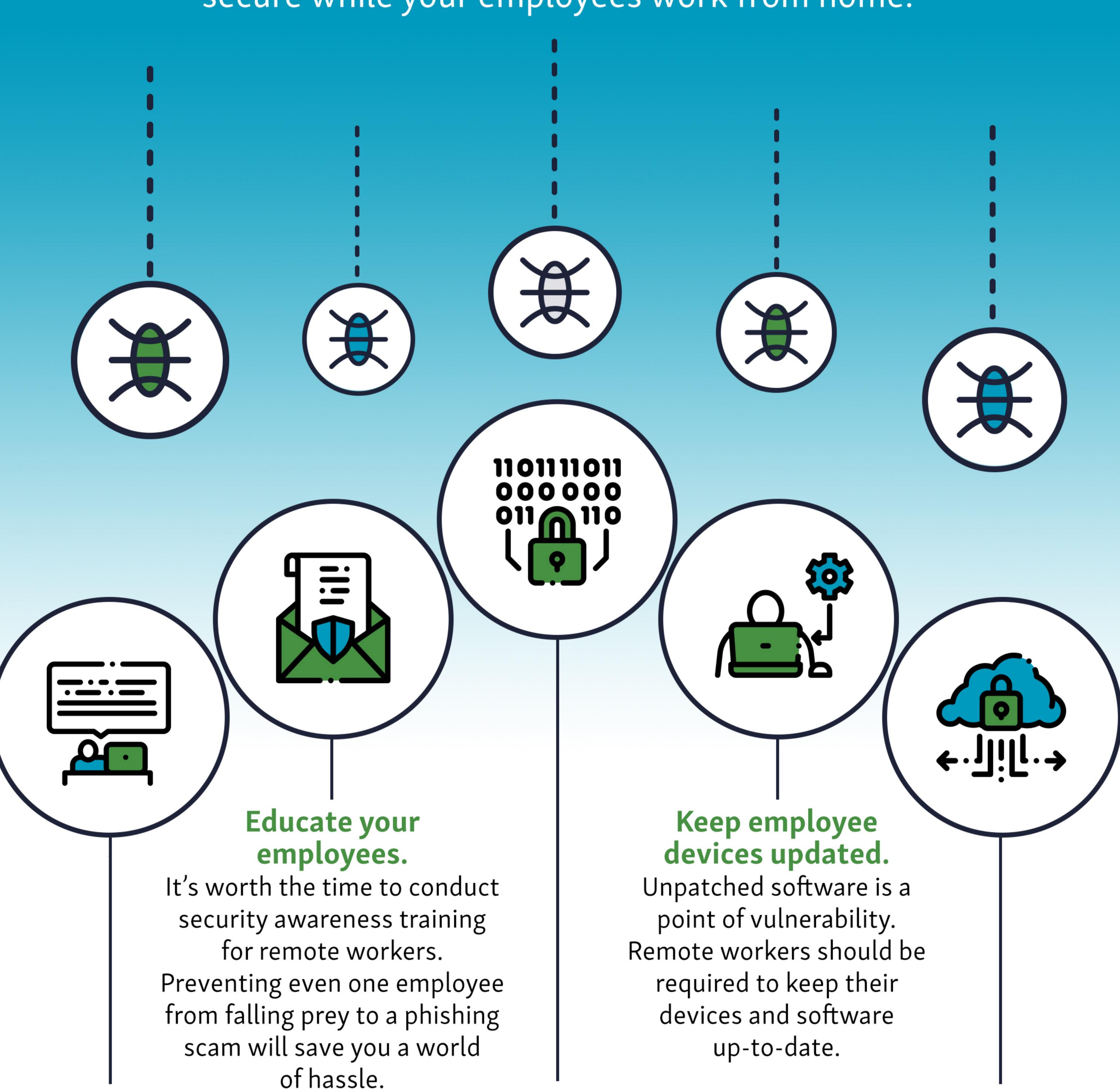


5 Best Practices FOR REMOTE WORK SECURITY

48%¹ of data breaches are caused by negligent employees or contractors. With employees working from home, cyber security risks are at a high. A recent survey by Imation² reported:

- 67% of remote employees break company security rules while working from home
- 41% of companies don't have a remote work policy in place that includes IT security

Security should be a top priority at a time when remote work is the norm. Here are 5 best practices to follow to keep your data and systems secure while your employees work from home:



Assess your remote work policies.

A policy created for partial remote work may not cover your needs for an entire work-from-home staff. Check that security is specifically addressed.

Use encryption.

Require end-to-end encryption for any communication between employees, and ensure all devices are encrypted.

Use a VPN.

Keep sensitive or mission-critical data secure by using a VPN. This allows remote workers to access the company network as if they were in the office.

With the right policies and practices in place, your remote workers can be just as secure as they had been in the office. Access One's experts are here to support your efforts to keep your systems and data secure – in all circumstances. Contact us today to learn more.

www.accessoneinc.com • info@accessoneinc.com • 800-804-8333