SONTIQ
A TransUnion® Company

REMOTE WORKERS BRING CYBERCRIME HOME (AND TO WORK)

REMOTE WORKERS ARE A CYBERTHREAT GATEWAY

- **80%** of security and business leaders believe their organizations face **more cyber risks** from **remote work**
- **34%** of remote workers say they follow **company security guidelines**
- **27% deliberately ignore** or circumvent **cybersecurity policies**
- **36% delay** applying **software updates**
- **92%** of organizations say **remote work** will be **permanent** in the next **two years**

SOURCE | Forrester, *The Rise of the Business-Aligned Security Executive*, 2020

How to Keep Your Business Safe Online

The weakest link in a company's security isn't technology; it's human error. In today's expanded virtual environment, companies and their employees are at greater risk. Cybercriminals are preying on human error — targeting remote workers with **phishing** and **ransomware** attacks to access and compromise employer systems.

In a **phishing attack**, a scammer sends an email designed to look like it's coming from a reputable organization or someone they know. The goal is to convince individuals to click on a malicious link, download malware, and/or reveal personal information. Phishing is now the technique used for the majority of ransomware attacks — with incidents **rising 110% in 2020**.

Ransomware is a particularly devastating form of malware that, once downloaded onto a device, encrypts and blocks access to sensitive files — often after the cybercriminals have stolen those files. The thieves then demand payment for victims to regain access to the data. **Ransomware increased a staggering 715%** during the pandemic, and in 2021 it was estimated a **new ransomware attack occurred every 11 seconds**.

85% OF DATA BREACHES INCLUDE A HUMAN ELEMENT

SOURCE | Verizon, *2021 Data Breach Investigations Report*

Finding and Fixing the Weakest Link

- **Bring Your Own Device (BYOD) |** Employees using their own devices often don't use smart passwords, keep software up-to-date, or install the latest security patches.
- **Bad password hygiene |** Weak password creation or the use of the same password across multiple sites means it's easier for cybercriminals to crack employee passwords than bypass advanced cybersecurity defenses.
- **Unsecure Wi-Fi networks |** Remote workers rarely strengthen their home network security or change their Wi-Fi router's default password, giving cybercriminals much easier access to company networks.
- **Phishing lures |** Cybercriminals are skilled at getting unsuspecting (or careless) individuals to click links and open attachments that can inject malware or reveal personal information.

TIPS FOR SAFER REMOTE WORKING

- **Provide training |** Give employees the tools and knowledge to work from home securely. Training should cover company-specific policies and basics like creating strong passwords and not conducting business over public Wi-Fi.
- **Automatic updates |** Have employees opt for automatic updates on their devices. As inconvenient as they may be, software updates are usually released to patch critical security vulnerabilities.
- **Safeguard internet routers |** Ensure each work-from-home employee sets up their router with a unique name and a strong password to prevent others from accessing their home Wi-Fi.
- **Set up multi-factor authentication |** Requiring two (or more) verification steps can prevent criminals from using exposed ID credentials to reset a supposedly "lost password" in the victims' name.
- **Password manager |** Cut down on the reuse of passwords across multiple sites by supplying employees with a password manager to store all their online login credentials in one secure location. Then they just need to remember one password to access their apps and accounts.
- **VPN |** Have employees connect to public and home Wi-Fi networks using a virtual private network (VPN) — especially when using mobile devices. Doing so encrypts online activity, ensuring security and privacy at both ends.
- **Adopt a zero-trust approach |** Remind employees to never click on links or open attachments from unverified accounts. If they get an unexpected request, especially one marked "urgent", they should look up the business's number online and call them to verify.

SONTIQ CAN HELP

We offer a full range of identity monitoring, restoration, and response products and services. We empower enterprises of all sizes, including the public sector and consumers, to be less vulnerable to the financial and emotional consequences of cyber threats and identity crimes.

ABOUT SONTIQ

Sontiq, a TransUnion company, is an intelligent identity security company arming businesses and consumers with a full range of award-winning identity and cyber monitoring solutions, as well as best-in-class restoration and response offerings. Sontiq products empower millions of customers and organizations to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Sontiq has an outstanding track record for delivering high-touch support and fraud remediation services, demonstrated through its 99% customer satisfaction ratings. https://www.sontiq.com

© 2022 Sontiq, Inc. All trademarks or trade names are properties of their respective owners. All rights reserved.