Remote workers can be especially vulnerable to phishing or voice-based phone call attacks since they are often responsible for their own security. An urgent SMS text message appearing to come from HR requested confirmation of your bank account for direct deposit. After clicking the link and entering your information, you later received an overdraft notice and a suspicious activity alert from your bank. You notified HR and learned that they did not send the request, so you contacted the security team and your bank.

Remote workers may not have access to a readily available in-house IT Team, automatic firmware, or patches, and may be working from older devices. A home wi-fi network may be less secure and cannot be protected by the company at all times.

Your supervisor notified you that company trade secrets were stolen from your work laptop and sold to competitors. An investigation revealed outdated software on your computer led to a vulnerability that allowed the hacker to gain access to this confidential data.

**Enable and use Multi-Factor Authentication whenever possible**

**Create a unique, long, and strong password made up of multiple words, often called a passphrase, for each account**

**Precautions, Risks, and Potential Outcomes**

**Security Precautions for your Home Office**

Did you know that working from home carries additional security risks?

- **42%** of U.S. labor force currently works from home full or part time¹
- **80%** of surveyed U.S. company leaders plan to let employees work remotely part time and **47%** full time long term²
- **20%** of businesses have faced a security breach in the last year due to a remote worker³

**RISK**

**WHAT COULD HAPPEN?**

- **Weak Passwords**
  - Easy to guess (e.g., birthdate, pet name, or common word)
  - Can be found in a dictionary

- **Social Engineering Attacks**
  - Phishing (email, phone calls, text messages)
  - Smishing (SMS text messages)
  - Smishing (text messages)

- **Outdated Systems/Software**
  - Products that are no longer supported or maintained
  - Software that is vulnerable to security exploits

**ADDITIONAL RESOURCES:**

- ZOMG it's ZOOM (SANS Webcast)
- OUCH! Newsletter: Virtual Private Networks (VPNs)
- OUCH! Newsletter: Securing Wi-Fi at Home
- OUCH! Newsletter: The Power of Updating
- OUCH! Newsletter: Social Engineering
- OUCH! Newsletter: Password Managers
- OUCH! Newsletter: Two-Step Verification

---


© SANS Institute 2021