Work from Home

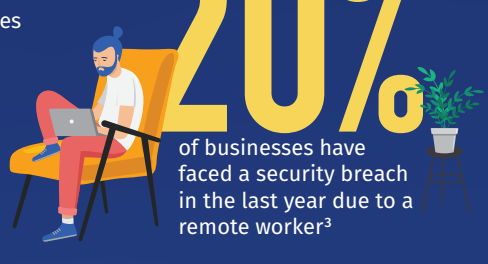
Precautions, Risks, and Potential Outcomes

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

42% of U.S. labor force currently works from home full or part time[1]

80% of surveyed U.S. company leaders plan to let employees work remotely part time and 47% full time long term[2]

20% of businesses have faced a security breach in the last year due to a remote worker[3]



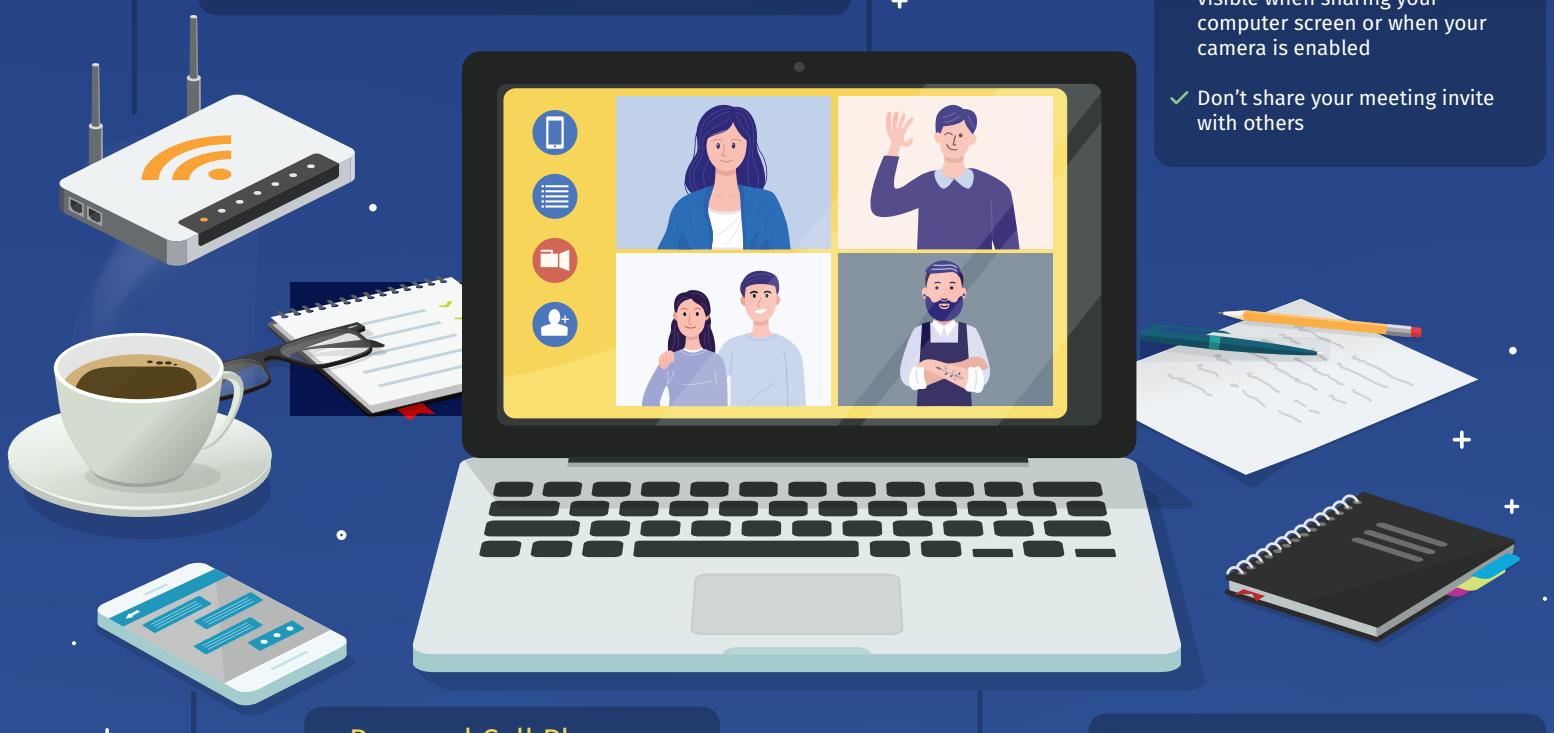
Security Precautions for your Home Office

Router

- ✓ Change the default admin password on your Wi-Fi Router to a unique, strong password
- ✓ Turn on automatic updating of your Wi-Fi Router's firmware
- ✓ Create a guest network for visitors and untrusted devices

Virtual Conferencing

- ✓ Only use authorized software for virtual conferencing and make sure it's always the latest version
- ✓ Make sure you don't have personal or sensitive information visible when sharing your computer screen or when your camera is enabled
- ✓ Don't share your meeting invite with others



Personal Cell Phone

- ✓ Keep your mobile device's operating system and apps updated
- ✓ Protect your mobile device by enabling screen lock
- ✓ Don't respond to any suspicious or urgent app and SMS text messages requesting that you click a link, send money, or share sensitive information
- ✓ Hang up immediately if you receive a suspicious or urgent call pressuring you to take some type of immediate action

Computer

- ✓ Enable automatic updating whenever possible on all your personal devices
- ✓ Quickly report and schedule a virtual meeting with IT if you suspect your system has been compromised; do not attempt to fix a hacked system
- ✓ Don't allow family members to use your work-issued device

VPN

- ✓ Never share your VPN information with anyone, such as your VPN passwords
- ✓ Make sure you follow your company's policies on properly using a VPN

Passwords

- ✓ 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

Top 3 Risks for Remote Workers:

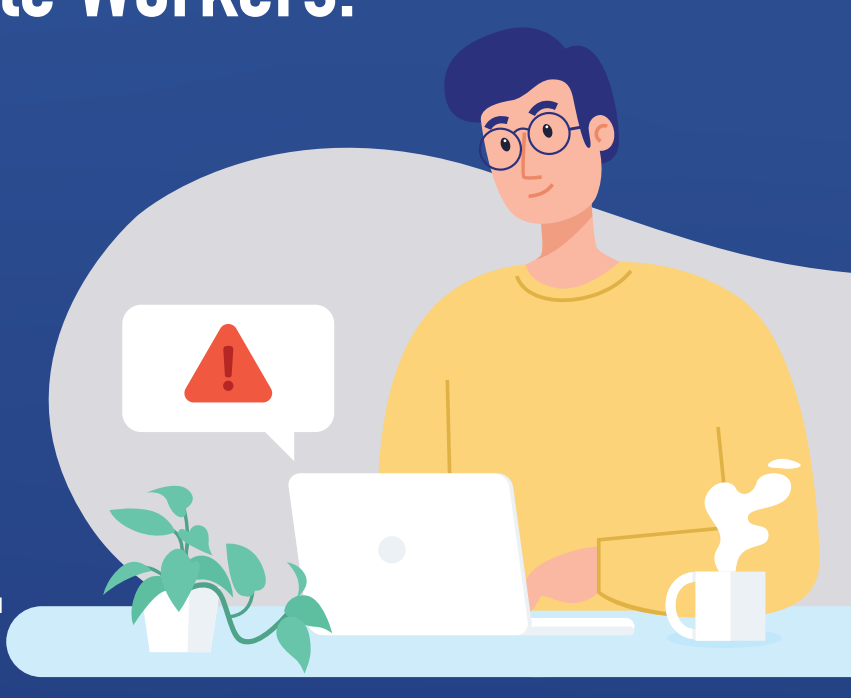
Weak Passwords

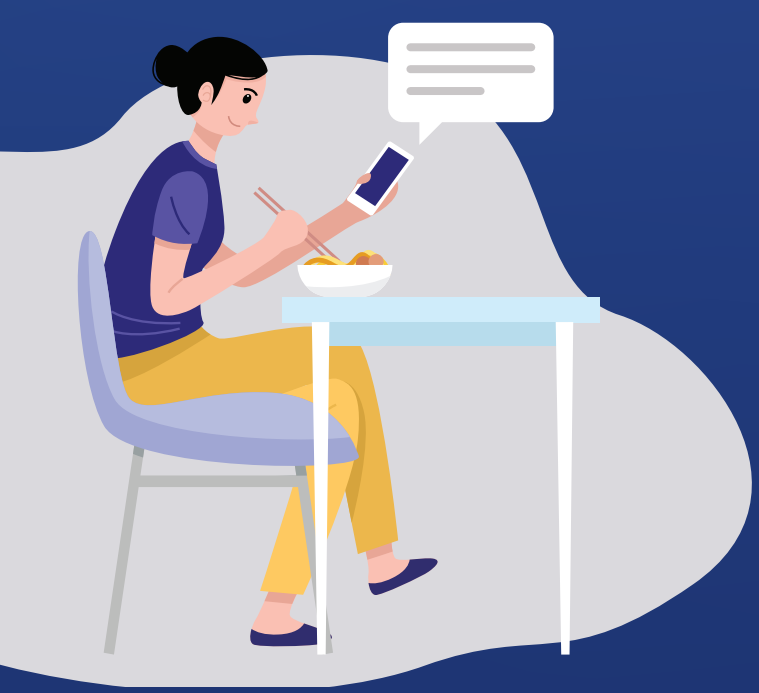
RISK

One of the primary drivers for breaches on a global scale. Short or obvious passwords, as well as using the same password for multiple accounts, can make you vulnerable to hackers.

WHAT COULD HAPPEN?

A coworker alerted you of a suspicious message sent from your email account. After escalating the situation to your security team, they informed you that your email account had been compromised due to a weak password.





Social Engineering Attacks

RISK

Remote workers can be especially vulnerable to phishing or voice-based phone call attacks since they are often responsible for their own security.

WHAT COULD HAPPEN?

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.

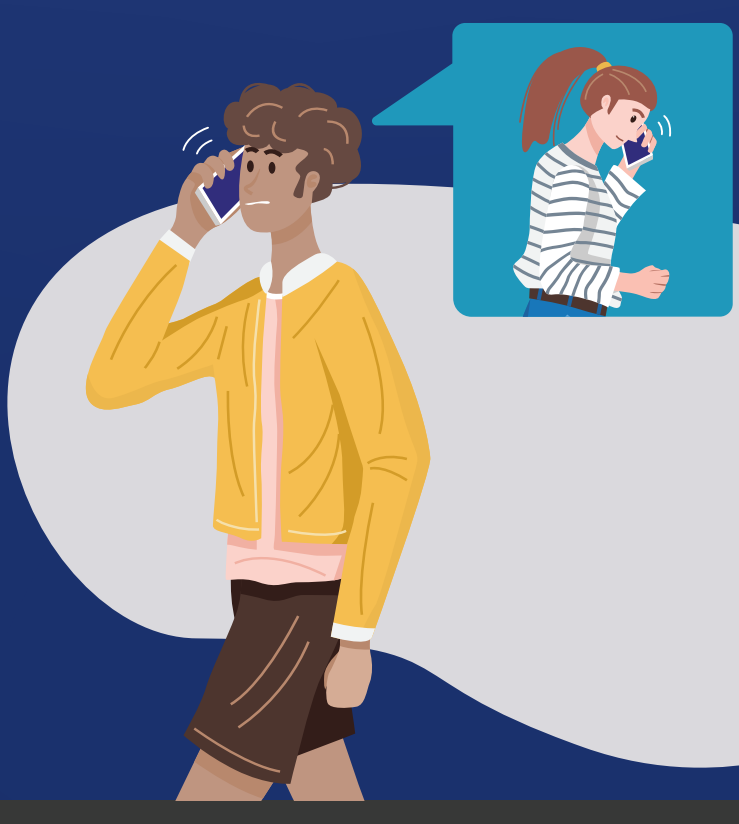
Outdated Systems/Software

RISK

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 can't be protected by the company at all times.

WHAT COULD HAPPEN?

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.



Citations:

1. Wong, May. (2020, June 29) "Stanford research provides a snapshot of a new working-from-home economy". Stanford News. Retrieved 2-26-21.
2. Golden, Ryan. (2020, July 16) "Gartner: Over 80% of company leaders plan to permit remote work after pandemic" HRDIVE.com. Retrieved 3-1-21.
3. Whitney, Lance. (2020, August 20) "How the shift to remote working has impacted cybersecurity". Techrepublic.com. Retrieved 2-26-21.

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 SECURITY AWARENESS