FACTSHEET

HIDDEN HOLIDAY RISKS

12 Ways to Avoid Data Security Issues When Working Remotely this Holiday Season

Remote working is on the rise and during the holidays, the 'out-of-office' workforce is at an all-year high.

Many employees who take time off still check their email and work on projects on the go throughout the holiday season, but certain work habits are putting confidential information at risk.

According to 2019 research[1] by Shred-it®,

47% of C-Suites and

31% of small business owners (SBOs) who experienced a breach **cited human error by employees or insiders as the main cause.**

Also,

94% of C-Suites and

79% of SBOs say that **flexible work arrangements are likely to become increasingly important over the next 5 years.**

Learn how to stay secure »

HIDDEN HOLIDAY RISKS: 12 WAYS TO AVOID SECURITY DATA ISSUES WHEN WORKING REMOTELY THIS HOLIDAY SEASON

Here are 12 ways remote workers can help keep the holiday season merry and bright—and secure.

1. **Minimize the amount of information stored on a mobile device** to only what is needed for work during the holidays.
2. **Update software and install patches immediately.** Research[2] has shown that 82% of discovered breaches occurred due to a failure to update software patches.
3. **Be alert when working remotely** in a coffee shop, airport lounge or bus. Put work away or change seats if anyone acts suspiciously.
4. **Do not post holiday travel plans or any identifying information** on social media websites.
5. **Never leave mobile devices unattended** in public or visible in a locked vehicle.
6. **Avoid sharing electronic devices with family, friends and other visitors.** Lock when they are not being used. Keep sensitive and confidential papers in a secure place too.
7. **Strengthen passwords on all devices and accounts** (long string of characters, incorporating numerals, letters, and symbols). Over 80% of hacking-related breaches leveraged either stolen and/or weak passwords.[3]
8. **Remember to log out of websites and accounts** especially when working on shared or public computers.
9. **Turn off Wi-Fi and Bluetooth connectivity when not being used.** To transmit anything confidential or connect to the office, use personal hot spots, a virtual private network (VPN) or password-protected Wi-Fi networks. Connecting by Bluetooth encrypts the data.
10. **Do not use unknown USB devices.** Only used company-approved devices.
11. **Watch out for phishing emails and malicious websites.** Signs include spelling and grammar mistakes, and urgent calls-to-action. Never send personal details such as names, address and credit card numbers over email.
12. **Follow company procedures for secure disposal of digital and paper information.** Do not put paper into the garbage or recycling container. Do not recycle end-of-life electronics devices or put them into the garbage. Bring them to the office for secure disposal after the holiday if possible.

Sources:
1. 2019 Data Protection Report, USA, Shred-it
2. Voke Media, Secure Operations Automation Market Snapshot report
3. 2018 Data Breach Investigations Report, Verizon

To learn more about best practices to stay secure through the holidays and beyond, visit **Shredit.com** or call **800-697-4733**.

Shred-it®