How remote working poses security risks for your organization

techrepublic.com/article/how-remote-working-poses-security-risks-for-your-organization

Lance Whitney

Companies are at greater risk due to phishing attacks, password sharing, and unsecured personal devices, says SailPoint.

Image: iStock/GaudiLab

The quick spread of the coronavirus triggered an equally quick transition toward a remote workforce among many organizations across the globe. But because of the abruptness of that shift, security has sometimes taken a back seat as organizations rushed to ramp up this new and evolving environment.

A report published Wednesday by identity management company SailPoint describes some of the key security risks posed by such a rapid change toward remote work.

For its report "The Cybersecurity Pandora's Box of Remote Work," SailPoint surveyed 9,000 people across six countries: the US, UK, France, German, Australia, and New Zealand. Asking the respondents if they've been working remotely since the start of COVID-19, the survey tried to determine the different security risks facing organizations as they've shifted to a remote work climate.

Among the 36% of US respondents who reported working remotely since the pandemic began, 79% said they've been working full time (30+ hours per week). The number of people working remotely was even higher in other countries, such as 51% in the UK, 49% in New Zealand, and 52% in Germany.

Phishing attacks

Almost half (48%) of the respondents in the US said they were hit by targeted phishing emails, phone calls, or texts in a personal or professional capacity during the first six months of remote work. That percentage was around the same, but in some cases higher, for the other countries covered in the survey. Further, 9% of those in the US revealed that they were hit by one or more such attack each week, a number that was slightly higher in several of the other countries.

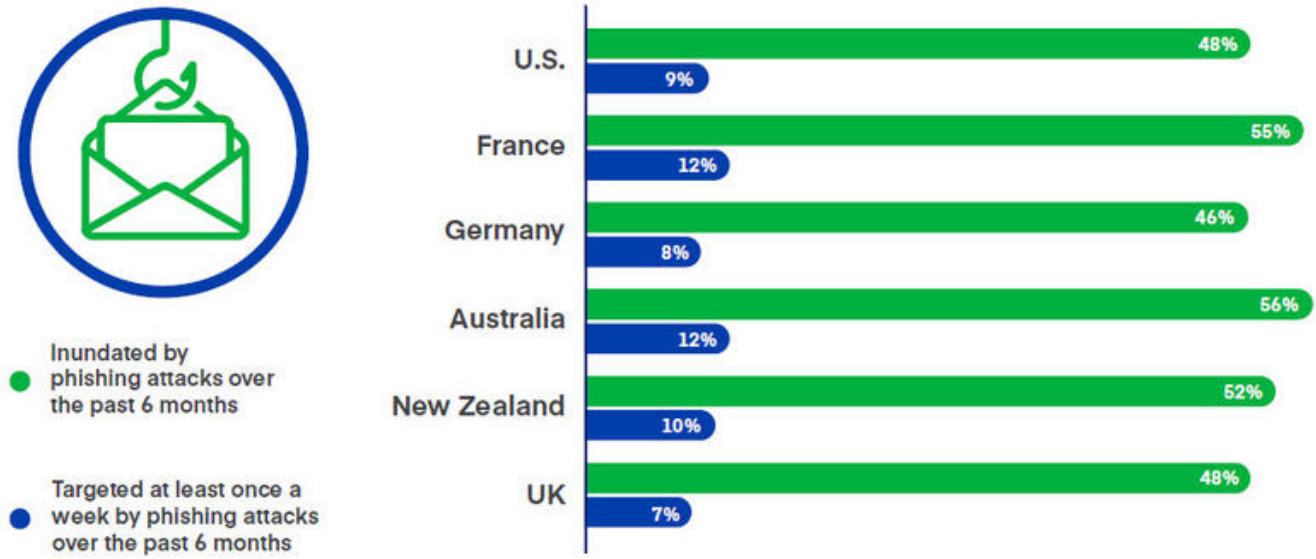

Image: SailPoint Technologies

"In the case of phishing, hackers target employees with malicious links embedded in carefully crafted emails," SailPoint CMO Juliette Rizkallah said in a press release. "Upon clicking, employees unknowingly download keylogging software onto their PC, providing their credentials to malicious actors. Hackers can then freely access important business assets and data, masquerading as a legitimate employee."

Password sharing

While working from home, some employees are prone to share passwords with other people as a way to accomplish certain tasks more quickly. Among respondents in the US, 23% admitted that they've shared work passwords with a third party, such as partners, roommates, and friends. That number was around the same in other countries but went as high as 25% in France and 26% in Australia.

Another pitfall is the failure to periodically change your password or a failure to even use a password. Among those in the US, 20% said they've changed their computer password over the past month. But 14% haven't changed their password in more than six months and 18% said that their computer isn't password protected in the first place.

In other countries, the percentage of computers that were not password protected was much lower, ranging from 2% to 4%. But the number of workers who hadn't changed their passwords in more than six months was much higher, ranging from 39% to 49%.

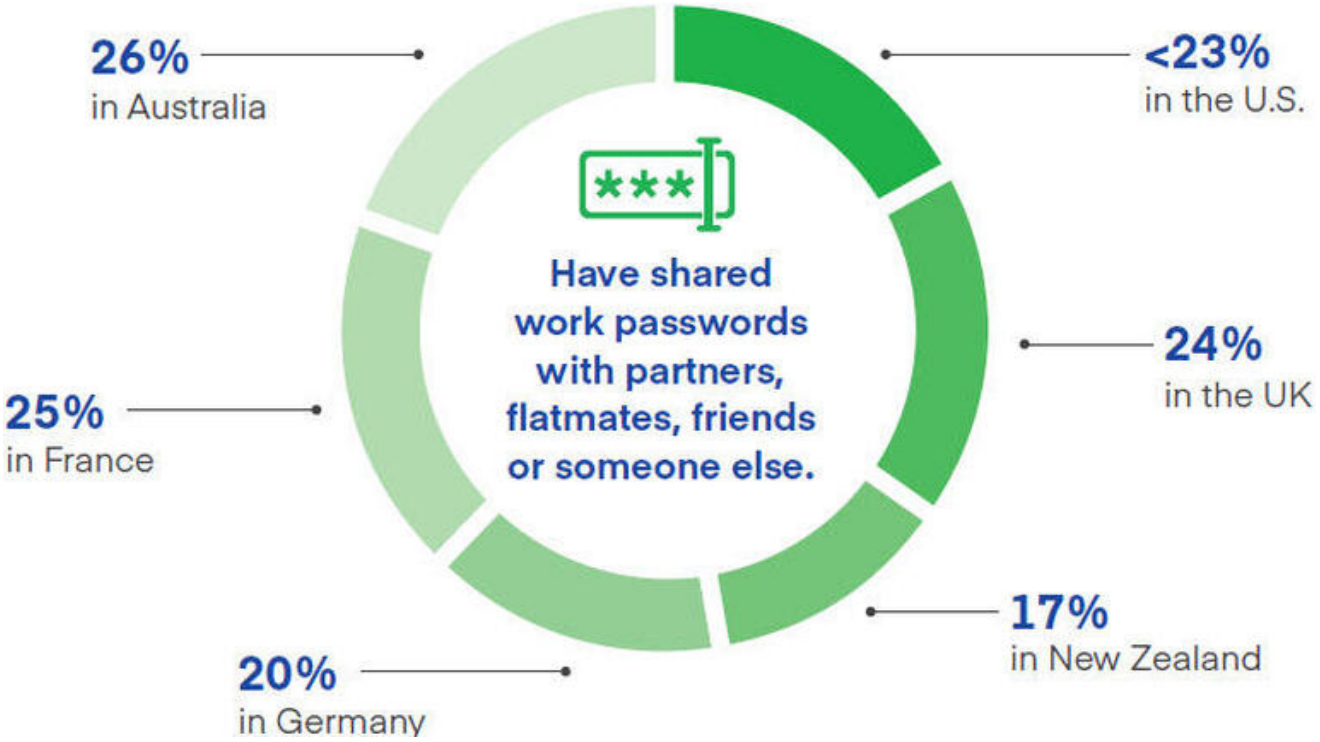

Image: SailPoint Technologies

"Sharing passwords across work and personal accounts can lead multiple systems to be compromised," Rizkallah said. "Once a hacker has those credentials, they can walk right into the corporate network. Access needs constant protection no matter how the workforce evolves; it is not enough to simply grant it."

Using personal devices

Keeping your personal and professional lives separate and distinct can be a challenge for people who work from home. That certainly applies to the devices being used. Among the US respondents, only 17% said they used devices owned and supplied by their employer. Results were different in other countries where half of the people surveyed said they use employer-supplied devices to work from home. However, a large percentage of remote workers in the European countries said they use their devices to check personal email and shop online.

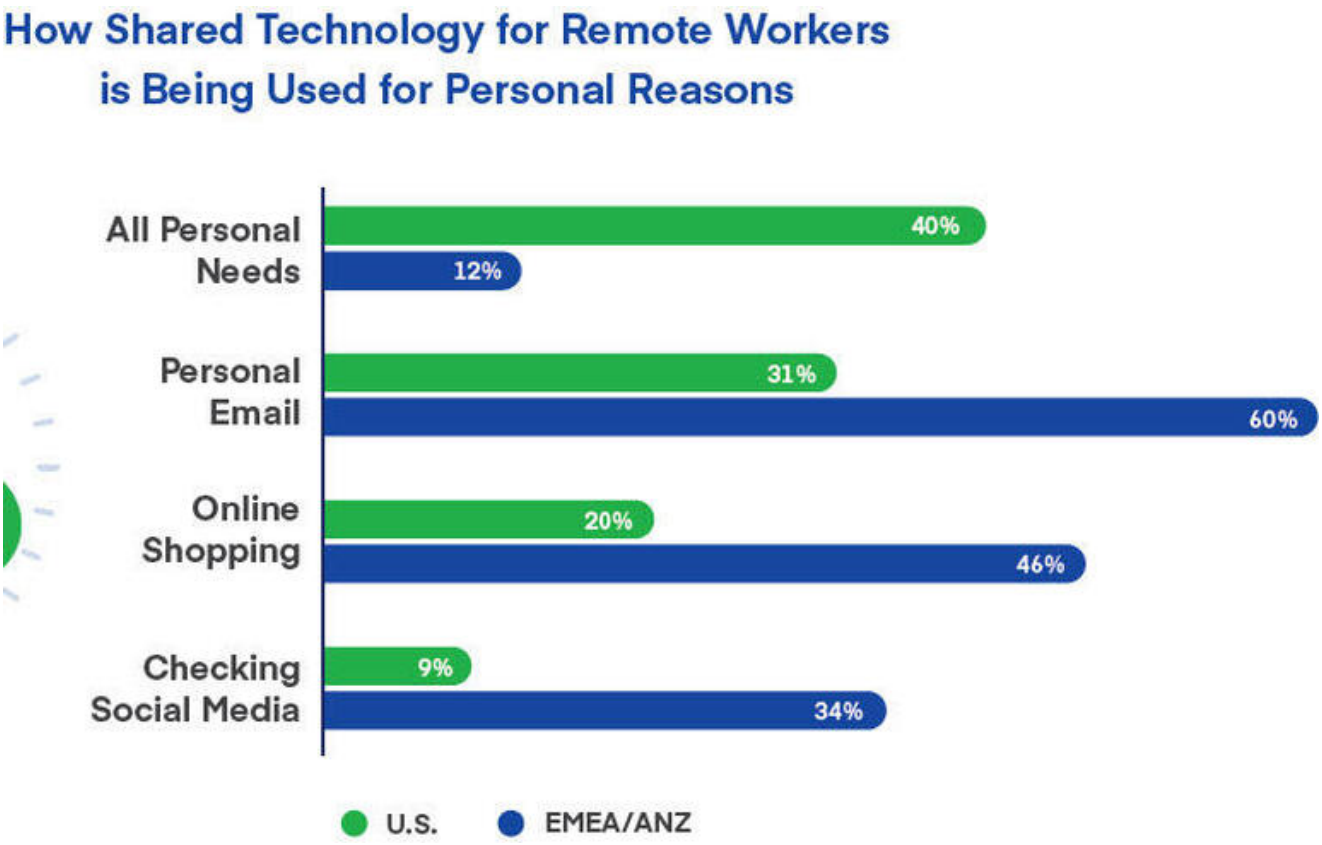

Image: SailPoint Technologies

"When the pandemic began, businesses had to flip a switch to enable remote work nearly overnight," Rizkallah said. "In this rush, many companies focused on granting access, skipping over the securing of that access. This resulted in an explosion of unsecured technology access across the business."

Recommendations

To help remote workers better secure themselves when working from home, SailPoint offers the following tips:

- Your password is like your toothbrush—don't share it and change it often. One in four respondents shared work passwords with a third party, including partners, roommates, or friends.
- Your Wi-Fi is your lifeline—don't log into unsecured networks. More than half of the respondents said they use unsecured public Wi-Fi networks.

- Your IT team is your best friend—use the tools they put in place, including multifactor authentication, security training, and VPN. Some 22% of those surveyed said they never use secondary verification to log into work applications.
- Your assumptions are an Achilles' heel—don't assume somebody won't hack you. Nearly half of respondents said they had experienced targeted phishing emails, calls, or texts in a personal or professional capacity during the first six months of remote work.