SailPoint

The Cybersecurity Pandora's Box of Remote Work

SailPoint

The Cybersecurity Pandora's Box of Remote Work

The transition to remote work opened a cybersecurity Pandora's box. While the human workforce always comes with a particular security risk level – due mostly to hackers leveraging targeted phishing tactics via email, text, and phone ad nauseam – COVID-19 shutdowns created a need for rapid enterprise technology implementation despite the risks involved. Consequently, the race to remote work blew Pandora's box wide open, creating an explosion of technology access across the workforce. This resulted in security and compliance gaps starting to surface, paving the way for potential data breach opportunities.

International research from SailPoint shows how real the cybersecurity threat is across today's digital enterprise. A distributed workforce means hackers can capitalize on the potential for unsecured workforce access across multiple user access points and the human element: password frailties and lax cybersecurity best practices.

The Catalyzation of The Distributed Workforce

As businesses kicked off 2020 with new goals for continued growth, many pushed forward under the assumption that their security infrastructure was sufficient. However, fast forward to the end of March, the world as we know it took an unprecedented turn as we collectively came under siege with the most significant public health crisis in a generation.

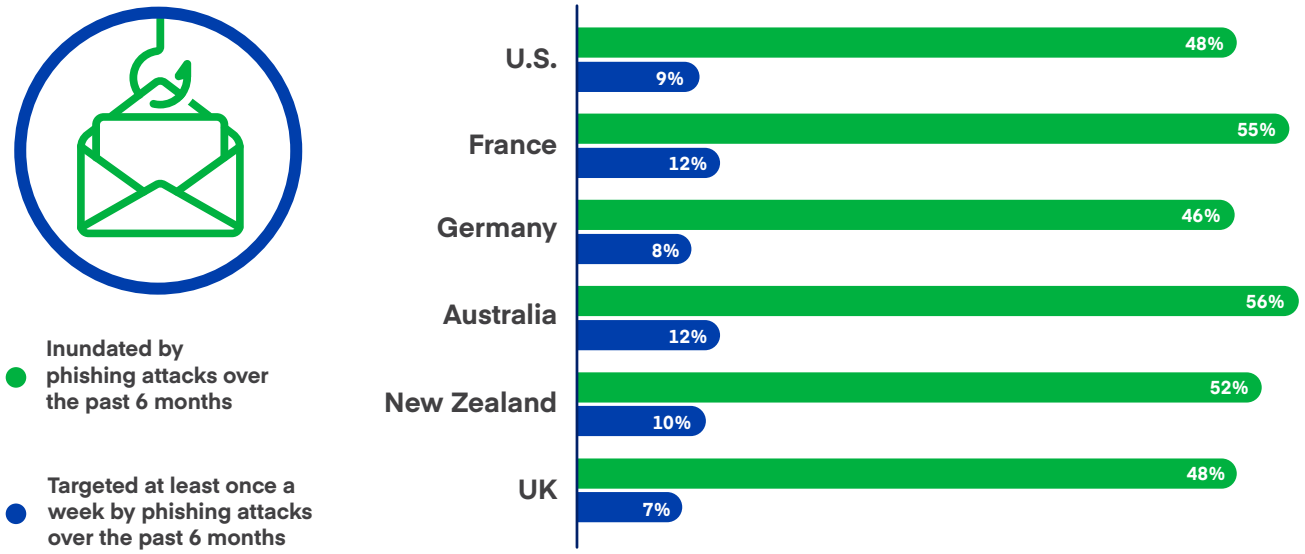
With COVID-19 blanketing the world and social distancing requirements put in place to help slow its spread, the pandemic had an immediate and catastrophic impact on global economies. Companies fortunate enough to remain open needed to shift their workforce to be fully remote. Working from home created an unrivaled digital acceleration that most did not expect, 97% of executives[1] agreeing that COVID-19 sped up digital transformation by six years.

Organizations quickly looked to supply their newly distributed workforce with the technology and tools necessary to sustain business continuity, with nearly half of all employees internationally reporting they had been working remote full-time as of March. Breaking that down further, of the **36% of total U.S. respondents** who reported working remotely during the start of COVID-19, **79% stated they were** employed full-time (30hrs+ per week). France, the UK, Germany, Australia, and New Zealand reported similar results, with **37% working remotely full-time** during the lockdown and an additional **12% working remotely part-time**.

The Total Number of Home Workers

[1]John Koetsier, "97% of Executives Say COVID-19 Sped Up Digital Transformation," Forbes, Sept. 10, 2020

A 100% remote workforce became a significant undertaking for enterprise IT teams. Many businesses inadvertently skimmed past some of the critical security requirements of remote work, like identity security, revealing the existing holes in security infrastructure and widening the threat landscape for cybercriminals. With every significant global crisis, bad actors look to take advantage of human nature with targeted scams, phishing, and vishing attacks. Hackers' tactics mean one of the largest threats posed to businesses today can be the employees themselves. **Forty-eight percent of total U.S. 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. Similarly, **over half of EMEA and ANZ respondents (51%)** experienced a phishing attack since the pandemic began, with **one in ten (10%)** reported a phishing attack targeted them once a week. Working from home lends itself to sharing sensitive company data and communicating important information via virtual platforms; it is a digital gold mine for hackers who own all the tools necessary to infiltrate a company when key defenses are down.



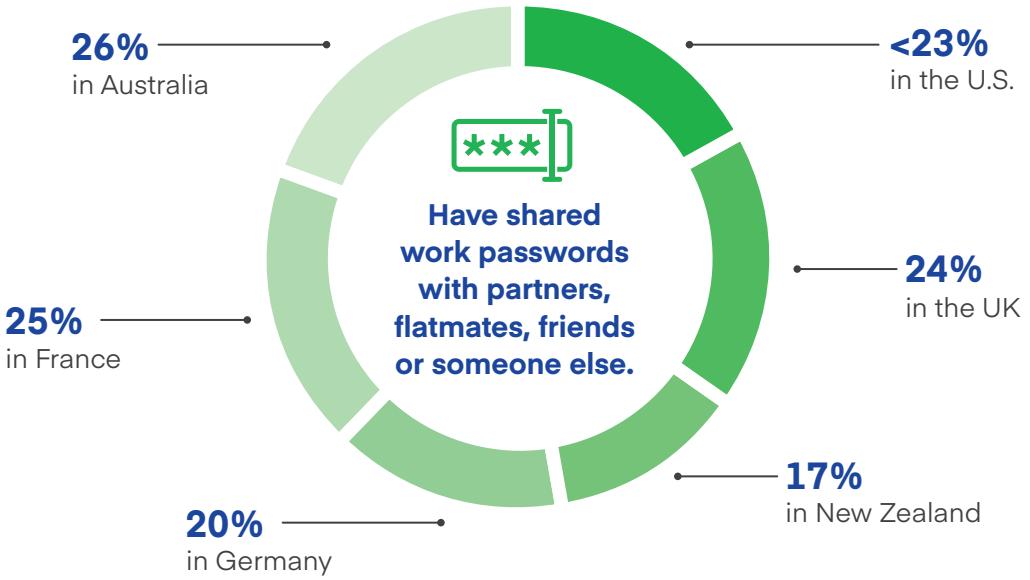
In addition to phishing tactics, SailPoint's research identified three cybersecurity doorways left opened as a result:

1. The Perils of Password Sharing

As the lines between home, work, and school fade, so too have the barriers in place to keep our personal and professional information secure. SailPoint's findings show, during the pandemic, password sharing become more commonplace within households. **One in 4 respondents internationally** shared work passwords with a 3rd party, including partners, roommates, or friends. In addition, **over half of total U.S. respondents** have not changed their work password(s) within the last six months, and **one-third (32%)** have not changed them in the previous six to even 12 months or longer. This trend holds true in **EMEA and ANZ, where only 23% of respondents** changed their work password, and **almost half (44%**) of respondents have not in over six months. Additionally, **roughly a quarter (23%)** of EMEA respondents have shared work passwords with a 3rd party, including partners, roommates, or friends.

Under the pandemic's personal, professional, and financial pressures, the human element of security has become more evident than ever. In this case, some users share work-related passwords to work faster, and some forget to change them as the to-do list gets longer. Sharing passwords across work and personal accounts can lead to multiple systems to be compromised. Once a hacker has those credentials, they can walk right into the corporate network.

Passwords are not the only shared work items.



	Changed password within 1 month:	Haven't changed password in over 6 months:	Computer isn't password protected in the first place:
U.S.	20%	14%	18%
EMEA	23%	44%	3%
France	23%	49%	4%
Germany	24%	39%	2%
Australia	21%	42%	3%
New Zealand	22%	45%	4%

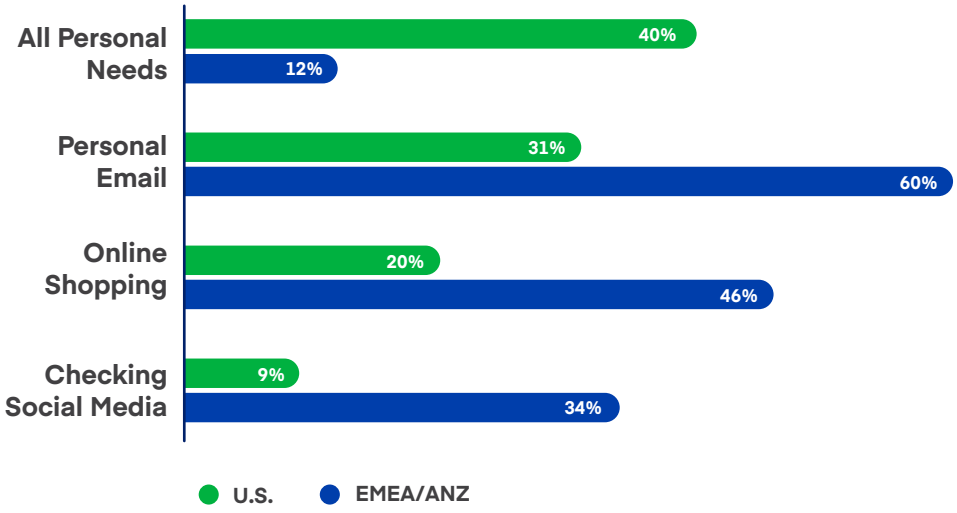
2. Personal Devices

Today's new remote reality demands make it clear that people wear more than one hat throughout the day – as a working professional, teacher, parent, caregiver, etc. As a result, device sharing with spouses, children, and other family members is a typical occurrence, as people try to stay connected during social distance requirements. Further, workers use these same technologies for different personal needs – such as checking personal email or social media channels and online shopping. Unfortunately, the cross-pollination of device use increases risk by creating multiple entry points and introducing new security vulnerabilities for all individuals and organizations involved.

SailPoint learned that **1 in 3 U.S. employees (33%)** stated that they use their own computer and smartphone to enable remote work, while only **17% use a computer and smartphone owned by their employer**. In EMEA and ANZ, **half of the employees** conducted remote work via employer-supplied technology.

As seen in the chart below, which compares how shared technology for remote work is being used for personal reasons, checking personal email is the clear front runner across all surveyed regions. This level of personal activity on devices used to conduct business and manage personal needs significantly increases the risk of hacking – especially when considering the increase in phishing scams. It only takes one reused password, unsafe connection, or click to hand hackers the keys to the kingdom – both the employees and the organizations. These actions introduce one of the leading reasons behind most security infrastructure vulnerabilities – human behavior.

How Shared Technology for Remote Workers is Being Used for Personal Reasons



3. The Human Element of Security

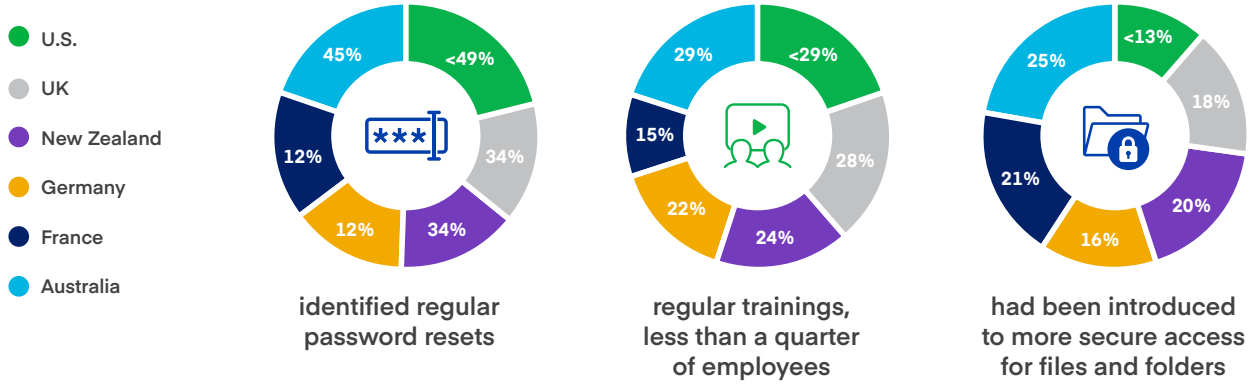
Human nature may vary person-to-person, but generational patterns have begun to emerge when considering security mindfulness as it relates to things like password sharing. In SailPoint's research, a clear generational divide was shown among full-time remote employees, with some regions having more significant differences between age groups than others. For example, in EMEA and ANZ, those below the age of 25 were shown to be the most at-risk internet users, being twice as likely to share their work-related password(s) with others. In fact, **over a third (39%)** admitted to password sharing, compared to **only a quarter (23%)** of all ages admitting the same. Across all age groups, **31% of 25-34 year old's, 27% of 35-40 year old's, 17% of 45-54 year old's, and 9% of over 55+** have admitted to sharing work passwords during the pandemic.

Similarly, in the U.S., nearly a **third (32%) of those under 25** admitted to sharing their passwords, but the most significant offenders were those **aged 25 to 34 (39%)**. As for the remaining age groups, the survey found that the older the group was, the lower the overall risk of password sharing. Specifically, those **35 to 44 (26%) and 45 to 54 (20%)** shared login credentials significantly less than their younger counterparts. But those aged **55-65+ were the most password secure**, with only **17% admitting** to swapping credentials.

Those **under age 25 in EMEA** are also less likely to change their passwords regularly, more likely to use personal computers for work, and tend to be less careful about using unsafe public WiFi – which is a consistent issue across nearly every age group in the U.S. **More than half of those under the age of 55 in the U.S.** admitted to 'sometimes' or 'never' avoiding public WiFi use while conducting business-related tasks. When considering this statistic through the lens of elevated password sharing, employees are opening up organizations to multiple attack vectors in the remote ecosystem.

Businesses Aren't Doing Enough to Protect Staff

When asked if there have been any workplace initiatives promoting staff cyber security protection:



Many organizations are operating under dated protocols and are severely lacking in the vital cybersecurity requirements demanded by today's standards. While table stakes protections like password resets, regular security training, and providing employees a more secure approach to accessing files and folders are important, organizations need to go a step further. A big challenge for most security pros is the lack of oversight regarding who has access, should have access, and what they are doing with that access. With so many new tools, platforms, databases, clouds, and everything else introduced rapidly to enable collaborative business continuity; organizations require scalable identity security solutions to protect what they cannot see. This is not about maintaining a certain level of control. It's about the intuitive enablement, management, optimization, and integration of software and computer systems through automation with A.I. and machine learning. Hence, workers automatically get the right access at the right time. In the meantime, security teams can ensure that all of their infrastructure, technology assets, and resources are safe and comply with identity and access policy.

Conclusion

The clear divide between work and personal environments is no longer cut and dried. We live and work in the same location, use a single computer or phone (or both) for all our needs, and allow our friends and family on the same devices we use for work, even sharing our passwords with our quarantine crew. Coupled with the explosion in access to technology across the business, the new M.O. of granting access at the drop of a hat without considering the broader security implications of that action left many organizations needlessly exposed. Businesses can't run without technology, and technology can't run securely without identity security. It is not enough to simply grant access to today's employees and expect that the business will stay secure – there is added risk exposure for all organizations with a remote workforce. Today's landscape has shown that identity security is a C-level priority, especially as we all prepare for the current and future state of operating in a primarily digital world. Security requires full commitment and compliance from every corner of the organization, and above all, it requires extra diligence from its people.

Methodology

SailPoint simultaneously deployed an international, statistically representative consumer survey across six countries in October 2020. The surveys were conducted among respondents over the age of 18 by 72Point across the United Kingdom (2,000 respondents), France (2,000 respondents), Germany (2,000 respondents), Australia (1,000 respondents) and New Zealand (1,000 respondents), and Dynata in the United States (1,000 respondents).

ABOUT SAILPOINT

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

SP1659-2011