SecurityAdvisor

Top Riskiest Behaviors and Employees in a Hybrid Workplace

Supporting the Human Firewall within Remote and Hybrid Organizations by Identifying the Riskiest Users and Their Most Dangerous Online Behaviors

Introduction

For the last year, remote and hybrid work environments have become permanent fixtures for many organizations. In 2020, more than 50% of US workers worked remotely full-time, and an additional 18% worked remotely part-time. Even as businesses begin to communicate their strategies for bringing people back into the office, major employers like Google, Microsoft, Salesforce, and others have indicated they will be adopting a permanent hybrid workplace to better accommodate their employees' needs.

While the flexibility of hybrid work is a boon to busy workers, this new work environment presents a significant cybersecurity challenge for security leaders. As remote and hybrid work environments become a permanent fixture for many organizations, businesses increase their human attack surface. In the absence of a physical office and an on-premises network, remote employees lose direct support from their organization's IT teams, making them more susceptible to cyberattacks.

The proliferation of cloud services that facilitate these remote and hybrid work environments fundamentally changes the nature of enterprise risk. While the cloud makes it easier for employees to access the tools and technologies needed for their jobs, users frequently connect to company systems via their home networks for remote access and use the same devices for personal tasks. This combination exponentially increases the threat landscape and makes humans the largest attack surface.

While it's essential to address these threats, imposing restrictions on browsing or access to specific websites hinders creativity, innovation, and even productivity. Instead, security leaders can empower their employees to identify and remediate cyberattacks by identifying the riskiest users and understanding which behaviors put organizations at risk.

Methodology

To better understand the type and volume of risky behaviors employees engage in as they work in their new remote and hybrid environments, SecurityAdvisor analyzed more than 500,000 malicious emails and an additional 500,000+ dangerous website visits by enterprise employees in more than twenty countries. Employees range from entry-level to executives and operate across many industries, including healthcare, financial services, communications, professional services, energy and utilities, retail, and hospitality. SecurityAdvisor then leveraged its patented technology to identify the riskiest users from the safest users.

The following analysis reveals the most common riskiest behaviors employees engage in regularly and who the most dangerous users are in a typical organization. The report concludes with critical suggestions for security leaders to improve employee behavior among their workforces.

Read on for a full breakdown of the report findings.

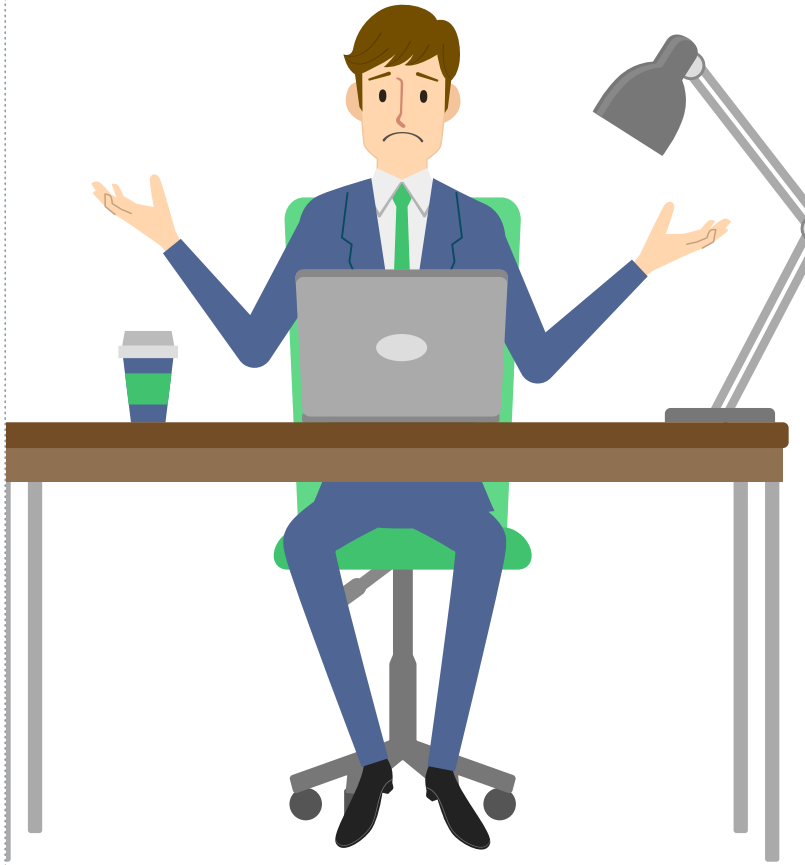
Five Most Common Risky Behaviors Employees Engage In

With the rise of hybrid work, the lines between work and personal life are blurred. While employees have always engaged in risky behaviors, they now use personal and work devices interchangeably and all hours of the day, which means their risky behaviors can significantly impact an organization's security.

Below is a breakdown of each of the most common online behaviors employees engage in that can lead to a data breach.

1. **Failing Logins and Forgetting Passwords:** Passwords are the front line of defense in protecting sensitive data. SecurityAdvisor's data found that the average person fails three logins per month. While multifactor authentication (MFA) provides extra protection against hackers, SecurityAdvisor found that 50% of users fail a multifactor authentication test every month, making it difficult for security leaders to differentiate between human error and malicious activity.

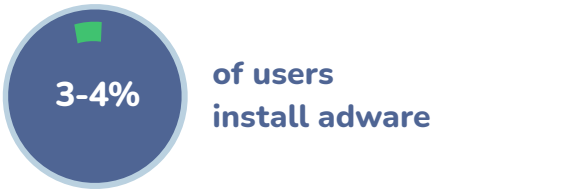
of users fail a multifactor authentication test every month



2. **Clicking on Phishing Emails:** Most spam filters can catch 99% of spam and phishing emails. Despite this high success rate, this means that 1% of spam and phishing emails will still end up in an employee's inbox. SecurityAdvisor data shows that the average employee receives five emails per month. In an organization of 5,000 users, this means 250 risky emails will bypass technology filters every month. The data also revealed that employees click on these phishing emails about 8% of the time. In a 5,000-employee organization, this equates to 20 phishing emails opened and clicked each month. These emails represent a potential data breach and security leaders should expect attack volumes to scale with the size of the organization.

3. **Installing Adware:** Adware is software that displays unwanted pop-up ads on a computer or mobile device. SecurityAdvisor found that 3-4% of users install adware, which often happens when installing untrusted software online, such as a free computer program or app. Without users' consent or knowledge, the download will include additional software containing adware that can spy and export data to malicious entities.

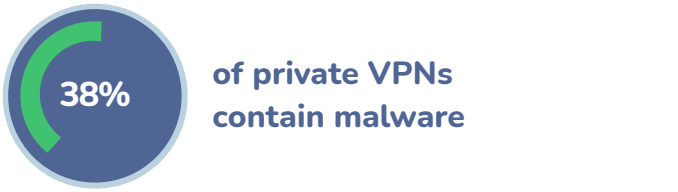
of the time, employees click on phishing emails



of users install adware

4. **Using P2P Software and Private VPNs:** As content becomes increasingly monetized by popular newspapers, websites, and studios, the number of tools that enable free access to content has also increased. For example, BitTorrent and Golden Frog allow users to share content, access content in restricted geographies, bypass paywalls, and download movies without being recognized. SecurityAdvisor found as many as 5% of employees install and use peer-to-peer (P2P) software or anonymizers. This situation represents a considerable risk to organizations as 38% of private VPNs contain malware, which can be used to bypass regular web filters, paywalls, and even national firewalls. Furthermore, 82% of private VPNs can read their clients' data. In remote and hybrid environments, this can include corporate data.

5. **Streaming Pirated Content:** Despite multiple controls, SecurityAdvisor data showed that 1% of employees in a typical enterprise find ways to watch pirated content through sites like Putlocker, VidCloud, or 123movies. These sites often are hotbeds for malware, ransomware, and keyloggers, which can even auto-install malicious software onto users' laptops with just one click.



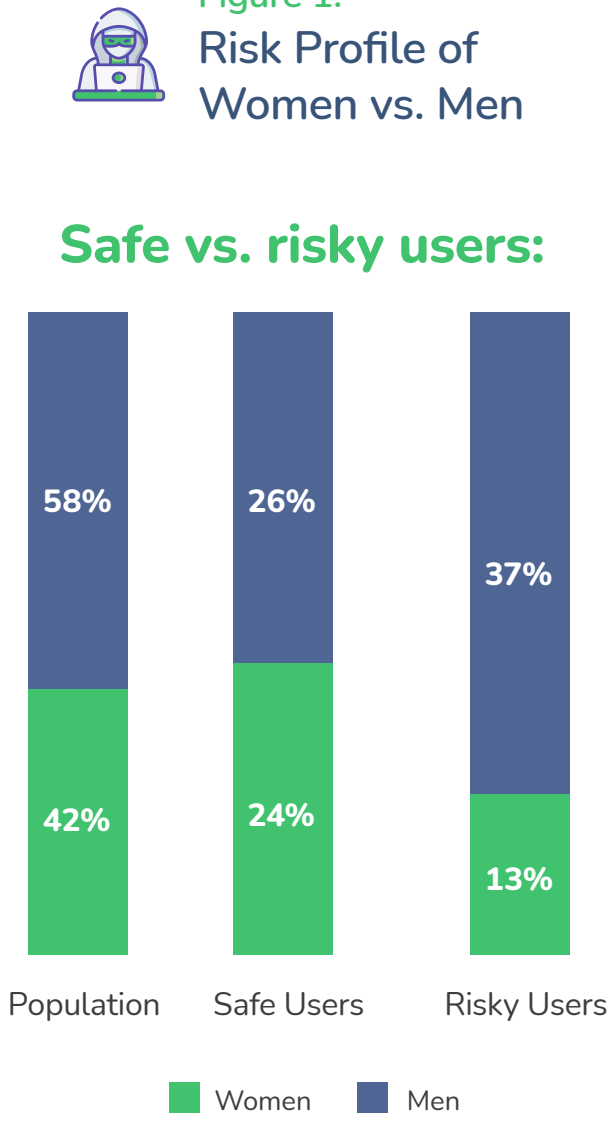
of private VPNs contain malware

Riskiest Employees: Men vs. Women

When it comes to online behaviors, SecurityAdvisor discovered that women are far safer than men. Despite the fact that women made up 42% of the sample data, they account for 48% of the top safe users and only 26% of risky users. Men, on the other hand, account for 74% of risky users.

A big driver of these risky behaviors stems from men's and women's online behaviors. According to SecurityAdvisor's data, men are more likely to visit dangerous adult websites, use P2P software, and watch pirated content than women.

Figure 1:
Risk Profile of Women vs. Men



Academic Insights on Men and Risk

Kellie A. McElhaney, Distinguished Teaching Fellow and Founding Director of Berkeley University's **Center for Equity, Gender, and Leadership (EGAL)** a leading expert on gender equity, provided some insight into some of the reasons behind the differences in data revealed between men and women. Contrary to popular belief, it is a myth that women are more risk averse than men. Both men and women engage in risky behavior. However, each gender tends to approach risk differently. Studies have proven that women are more aware of the long-term ramifications of a potentially risky behaviors when compared to men, particularly when it comes to negative consequences. Men, on the other hand, look at risk as a game. They are trained at an early age to win at all costs and, when threatened with a loss or negative outcome, they will do whatever they can to turn that potential loss into a win. The reason for this is that the penalties for taking a risk and failing are far less severe for men than they are for women – or anyone else who is not a part of the dominant group in a society.

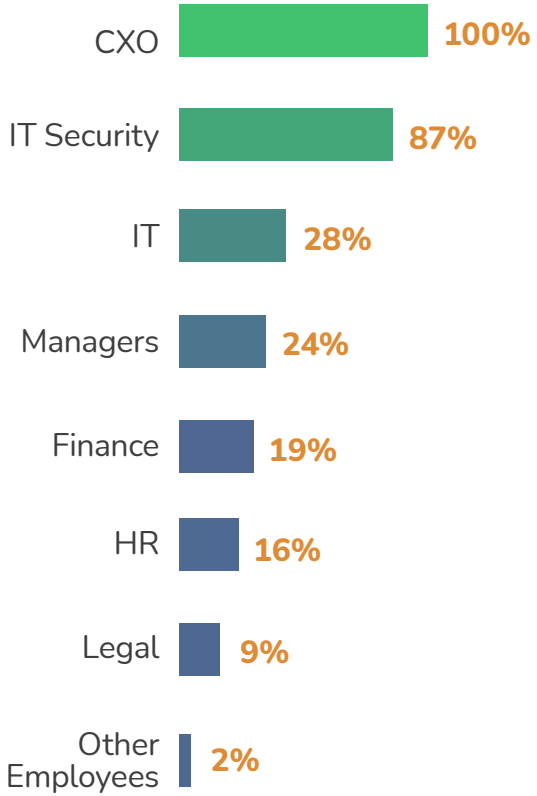
Riskiest Employees: Role and Seniority

Conventional wisdom states that junior employees represent the riskiest users in a typical organization. The reality is that risk is a function of both behavior and whether cybercriminals target the individual. While any individual can be a phishing target, malicious actors purposefully target employees who have privileged access to certain sensitive information, which varies by their role in the organization and department.

SecurityAdvisor's analysis revealed that senior-level employees, including members of the C-suite (CxOs, are targeted by phishers almost 50 times more than an average employee. This makes C-level executives inherently riskier and more vulnerable to cyberattacks. The chart below illustrates the frequency of cyberattacks that target CxOs compared to other employees.

Figure 2:

Most Popular Phishing Targets by Volume



Frequency of Risky Behaviors

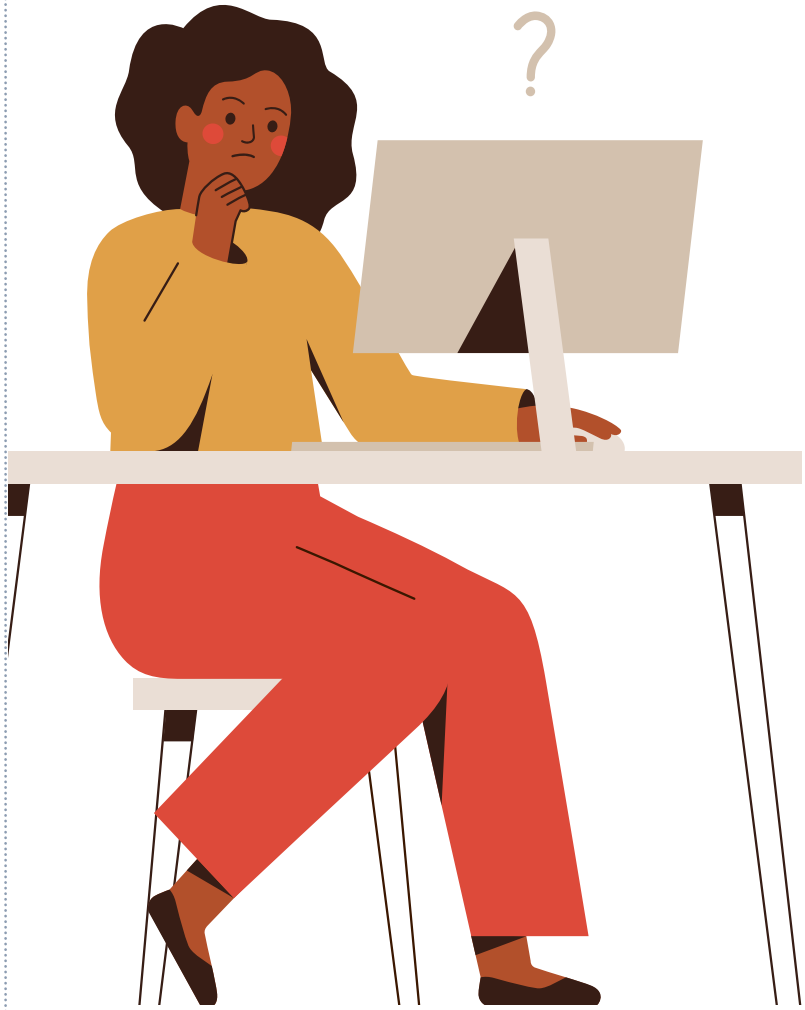
Everyday, Employees perform hundreds of tasks, from responding to emails and collaborating with coworkers to conducting online searches and logging into corporate systems. While only 1% of employee activities are risky, each risky action represents a potential data breach or large-scale disaster for organizations – and these actions happen multiple times a day for any organization.

During the holiday season, for example, employee engagement in risky activities increases. SecurityAdvisor found that risky online activities increased by almost 60% during the holiday season because employees have more time to indulge in recreational activities, such as watching pirated movies or shopping on compromised websites.

Positively Changing Risky Employee Behavior Through Personalized Coaching

The rise of hybrid work has undoubtedly changed the cybersecurity landscape. By increasing online access to tools and data, organizations are exposed and leave themselves vulnerable to the consequences of their employees' online behavior.

While employee risk will never go away entirely, employees can be coached to become the best defense line for their organization. Consistent and personalized education can help people avoid risky behaviors and measurably reduce security incidents by 70%, showcasing the power of the "human firewall." By coaching employees on their unique behaviors, they can better understand which behaviors pose risks to their organization and take proactive steps to address these threats.



Permanent behavior change does not happen overnight. Psychologist ermann Ebbinghaus discovered that long-term behavior change comes from consistent training and engagement. The average person requires constant reminders to apply knowledge at the right moment. To effectively change behaviors, security leaders need to provide specialized guidance about each threat when an employee engages in risky behaviors. This education should also be personalized for each employee's aptitude, susceptibility to threats, job role, and department to ensure education is relevant.

SecurityAdvisor helps companies strengthen their organization's human firewalls by providing personalized microlessons that facilitate positive individual behavior. For more information on how to positively change risky employee behavior and quanti iably reduce security incidents through personalized, real-time coaching, please visit securityadvisor.io.