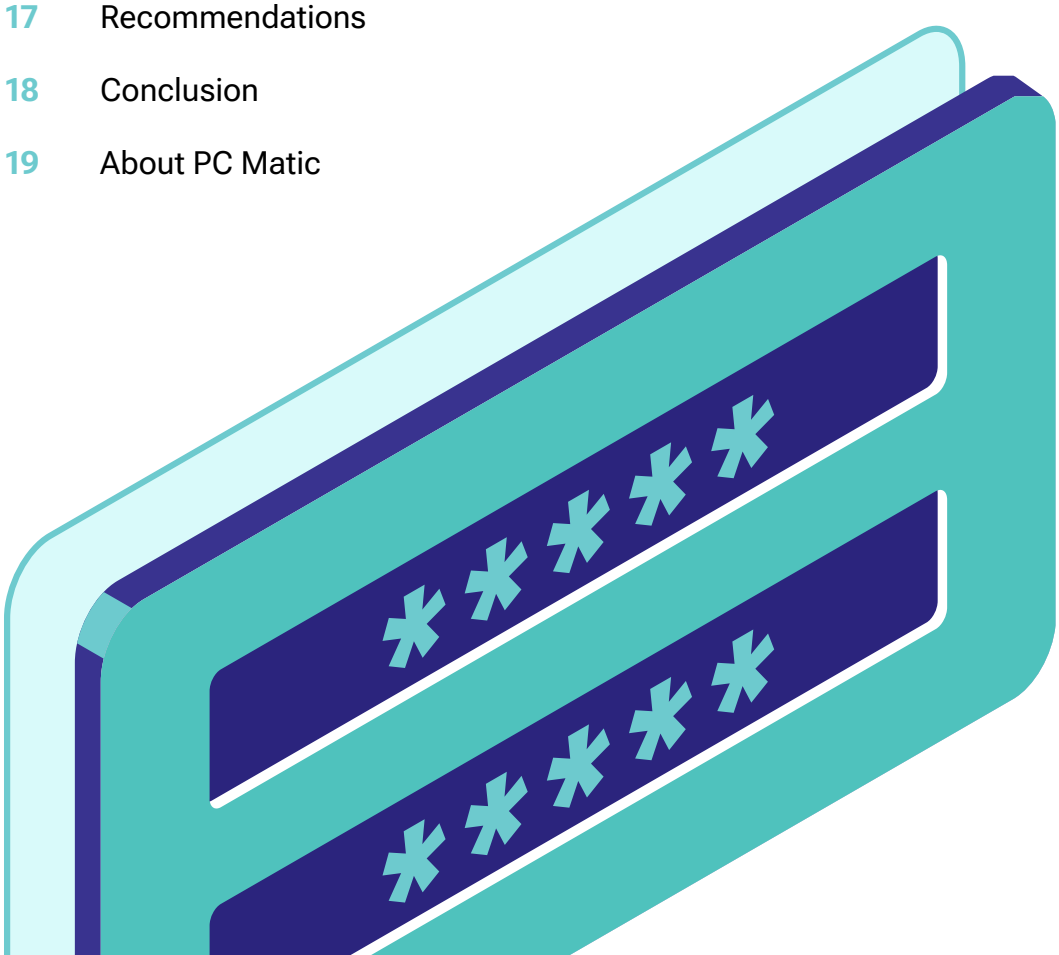
2022 Password Hygiene & Habits Report

PC Matic

TABLE OF CONTENTS



FOREWARD

As the nation transitioned back to in-office work environments, and as more and more remote workers continue to login from home, the last year has been a particularly interesting time for cybersecurity.

Whether it be cyber attacks on various components of critical infrastructure in the United States – including food distributors and an East coast oil pipeline – IT professionals have been faced with unprecedented challenges as cybersecurity threats continue to evolve at an alarming speed.

Despite the challenges and growing pains of the last year, one thing remains true – America and its reliance on technology continues to grow. With this, comes the growing threats of cybercrime, and the ramifications these crimes have on consumers, businesses, the U.S. economy, and the national security of our Nation.

As cybersecurity professionals are faced with these challenges, PC Matic recommends the most secure technology, like our default-deny approach, to combat cybercrime. In an effort to better understand American cybersecurity infrastructure, we've taken another deep dive into a major loophole. Our team wanted a more in depth understanding of password habits and hygiene. So, for the fourth year in a row, we conducted a survey to find out more about how Americans understand and use passwords.

To better understand this topic, our team surveyed over 1,085 individuals to gain insight into their security habits, and more specifically, their password hygiene. In our research, we looked at things such as how frequently users change their passwords, whether employers allow employees to choose their own passwords versus issuing them to employees, and what types of additional security layers individuals and their companies are using to combat cybercrime.

Passwords might seem like a minor detail, but our research confirms password hygiene is a growing threat. Individuals' personal information along with trade secrets of businesses across the globe need protecting. The explosion of ransomware in the past year and a half is proof enough of that.

This report, and the data standing behind it, aims to provide you with specific information related to the password hygiene and habits of Americans. Further, this report outlines steps that can be taken to combat cybercrime, regardless of whether you're an individual, a government, or a small or large business.

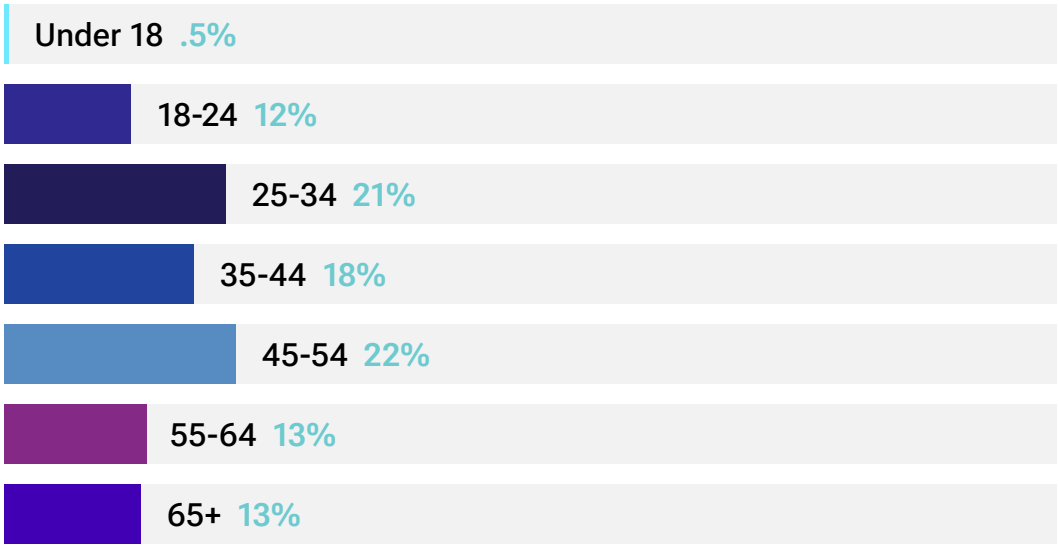
Cybersecurity is growing in importance across the globe, and we are eager to share with you what we have learned from our research and analysis in this report.

METHODOLOGY

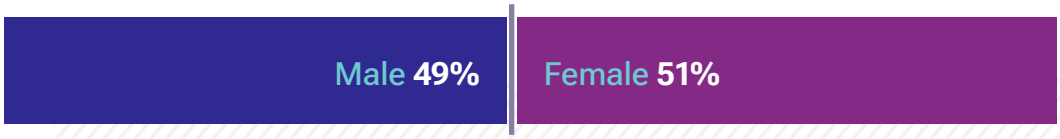
The information gathered within this report was obtained by surveying approximately 2,500 individuals in May 2021 regarding their cybersecurity practices, specifically those habits surrounding password protection. The respondents included both male and female adults, located throughout the United States.

The goal of the survey was to create a baseline for security practices used by individuals throughout the nation, regardless of their age, gender, educational background, and/or employment experience. PC Matic was able to establish this baseline with the data provided by survey respondents.

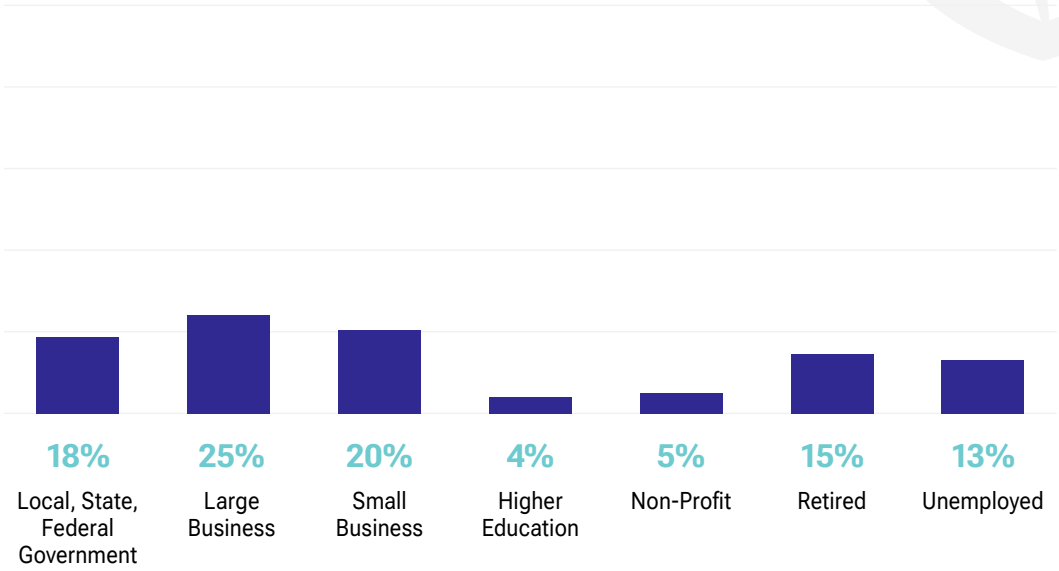
AGE



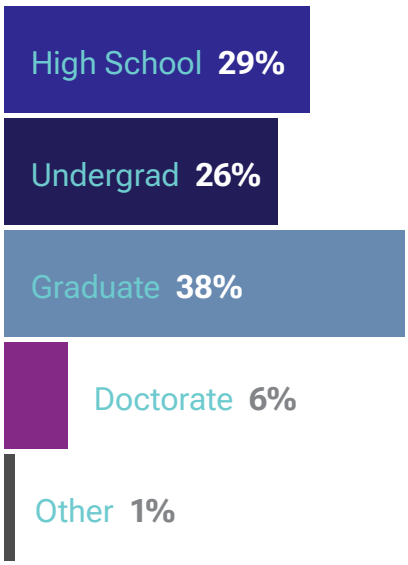
GENDER



JOB STATUS



EDUCATIONAL BACKGROUND



PASSWORD CHANGE FREQUENCY

Results from survey respondents confirm that Americans still continue to struggle with password management. This poses a significant threat for a number of reasons. First, passwords serve as our so-called "digital keys" to personal banking websites, email accounts, social media platforms, and even credit monitoring services. Even more so, we use passwords to protect sensitive information on company servers and to access corporate networks. It is incredibly important to keep passwords safe, and when considering the poor management practices by respondents – cybersecurity threats are present amongst us.

Two years ago, in our 2020 survey, nearly 70% of respondents indicated that they had more than one email account. That number rose sharply to 87% in our 2021 survey, and stayed relatively consistent this year with 86% of respondents indicating in our 2022 survey that they have more than one email account.

That considered, of those who responded that they have at least one e-mail account or more, 31% of respondents indicated that they aren't sure when they last changed their password or never have at all. This is up 4-percentage points from our 2021 survey.

When looking into how individuals keep track of their passwords, just under 40% of respondents indicated that they remember their passwords by memory, and don't use a password manager or write them down somewhere. This is down slightly from 41% in our 2021 survey.

Considering nearly 40% of Americans remember their passwords by memory, we're led to believe two things. First, it leads us to believe that this is why such a significant percentage of respondents haven't changed their passwords or don't know when they last did. Second, it also continues to lead us to believe that they're using the same password for multiple accounts and that their passwords likely don't meet complex password standards.

As stated in both our 2020 and 2021 report, if users are forced to update passwords regularly and meet certain complexity measures, the likelihood of them maintaining the ability to mentally store their password significantly diminishes, and that is a good thing for password hygiene and cybersecurity in general.

HOW MANY EMAIL ADDRESSES DO YOU HAVE?

1: **14%**

2: **37%**

3: **21%**

4+: **28%**

WHEN WAS THE LAST TIME YOU CHANGED YOUR EMAIL PASSWORD?

Within the last month: **30%**

Sometime this year: **39%**

I'm not sure: **26%**

Never: **6%**

HOW DO YOU REMEMBER YOUR PASSWORD?

IN MY HEAD

39%

WRITTEN DOWN

31%

PASSWORD MANAGER

30%

PASSWORD STORAGE

As with results from our 2020 survey, our 2021 survey reconfirmed that as individuals grow in age, they are more likely to write their passwords down. Respondents in 2022 confirmed that as well with 47.26% of baby boomers preferring to write their passwords down and only 22.03% of millennials preferring to do so. It is important to recognize that our millennials finding is up by nearly 5% since our 2021 survey.

Millennials, like in our 2021 survey results, continue to lead the respondent groups in both remembering their passwords by memory and in the utilization of password managers. Nearly 45.44% of millennial respondents indicated that they remember their passwords by memory and just over 32% stated that they use a password manager.

Password Manager Utilization is on the Rise

In our 2020 report, we reported that only 19% of survey respondents utilized a password manager tool. In 2021, our results showed nearly 30% of respondents utilized a password manager to safeguard their password information. This number remained virtually unchanged with 29.72% of respondents indicating they use a password manager tool.

Using a password manager is a good strategy, but, as we've pointed out in previous reports, it is important to recognize that using the tool could put user information at greater risk if not implemented properly.

For example, if a user safeguards all their passwords in a password manager, and their password manager is compromised, all of their personal information and passwords are now accessible. To make these tools more secure for those who choose to use them, it is imperative that multi-factor authentication be deployed as another layer of security in safeguarding users and their sensitive information.

SETTING PASSWORDS

Passwords should be complex – but picking them out doesn't have to be. Passwords should be a combination of upper and lower case letters, numbers, and special characters. Users should never reuse passwords on multiple accounts and should create unique passwords and store them in a safe place for remembrance.

Let's Talk About Corporate Passwords

In regards to corporate passwords, we strongly recommend that businesses issue passwords to their employees. That said, up from 16.36% in our 2021 survey, our 2022 survey still found that only 20.54% of employers issue their employees a password. The overwhelming majority of employers, 75.9%, still allow their employees to choose their own passwords while just 3.6% of employees have their passwords set by a password generator.

Yes, issuing passwords to your employees isn't an easy task. However, issuing passwords, although harder, cuts down on the ability of employees to reuse personal passwords and minimizes the risk of cybercriminals gaining access to corporate networks via compromised passwords.

If the business doesn't have the resources to issue passwords to its employees there are a number of password management tools that can automate this process for you. Regardless, removing the ability of the employee to choose their password vastly reduces risk for the business. It is also imperative that you frequently change these passwords as well.

ADDITIONAL SECURITY PARAMETERS

Year over year, as we conduct our research on password habits and hygiene, respondents continue to confirm that they aren't managing their passwords properly. This leads one to ask: are users taking additional security measures to offset the lack of password hygiene?

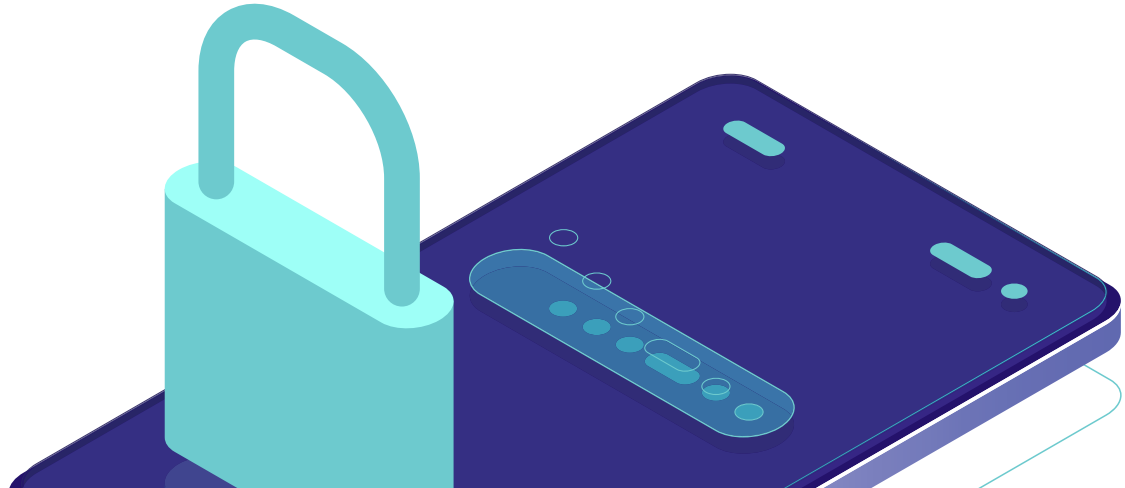
Additional steps users could take may include the use of virtual private networks (VPNs), deploying multi-factor authentication (MFA), and securing WiFi connections.

Password Lockout Thresholds:

In our 2020 report, we outlined that nearly 45% of respondents utilized the password lockout feature on their personal computers. In last year's results, we saw a sharp decline to only 30% of users utilizing this feature, and we attributed that decline to a possible decrease in the number of respondents who use personal computers as more and more users adopt tablets and mobile devices. Our 2022 results showed a marginal increase to 33% of respondents utilizing this feature.

Those who indicated they utilize the password lockout feature on their work computer ticked up slightly from 12% in 2021 to 12.75% in our 2022 results. Results of those who indicated they use the password lockout feature at both home and work remained virtually unchanged from 2021 to 2022, with 39.8% of respondents indicating they use the feature.

Users who do not utilize the password lockout feature slightly decreased year over year from 20.6% in 2020 to 17.5% in 2021. This trend continued from 2021 to 2022, with 15.4% of users now saying they don't use the feature.



DOES YOUR COMPUTER REQUIRE A PASSWORD TO REGAIN ACCESS AFTER A PERIOD OF INACTIVITY?

2020

Yes, my personal computer: **45%**

Yes, my work computer: **9%**

Yes, both my work and home computer: **26%**

No: **21%**

2021

Yes, my personal computer: **30%**

Yes, my work computer: **12%**

Yes, both my work and home computer: **40%**

No: **18%**

2022

Yes, my personal computer: **33%**

Yes, my work computer: **13%**

Yes, both my work and home computer: **39%**

No: **15%**

How Secure Are Home Wi-Fi Networks?

When your internet service provider comes out to your home to set up your internet service, they likely provided you with a Wi-Fi password. If not, the home or business where you're connected likely was asked what they'd like the password to be. In 2020, we found that more than 53% of surveyors hadn't changed their password since the Wi-Fi had been initially set up. 2021 results found that nearly 60% of users aren't changing their Wi-Fi passwords or don't know how, and our 2022 results found that this number is back on par with 2020's numbers, with 54.58% of respondents in the same manner.

IS YOUR WI-FI CONNECTION PASSWORD PROTECTED?

Yes: **89%**

No: **3%**

I'm not sure: **7%**

HOW FREQUENTLY DO YOU CHANGE YOUR WI-FI PASSWORD?

2021

I don't know how to: **8%**

Monthly: **18%**

Annually: **23%**

Not since setup: **41%**

Never: **10%**

2022

I don't know how to: **9%**

Monthly: **22%**

Annually: **23%**

Not since setup: **37%**

Never: **9%**

GROWTH IN AWARENESS

IN OUR FIRST PASSWORDS HYGIENE AND HABITS REPORT, CONDUCTED IN 2019, 20% OF RESPONDENTS DIDN'T KNOW WHAT A VPN WAS. IN 2021, ONLY 8% OF RESPONDENTS INDICATED THEY DIDN'T KNOW WHAT A VPN IS. IN 2022, ONLY 6% OF RESPONDENTS INDICATED THAT THEY DIDN'T KNOW WHAT A VPN IS.

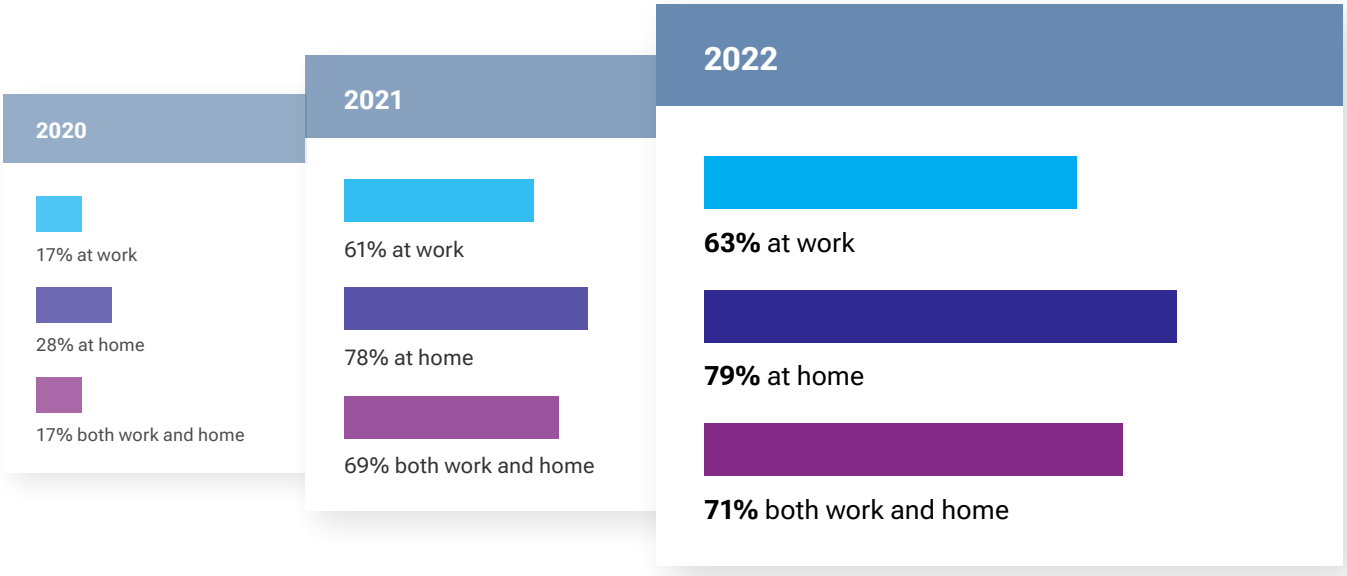
Utilizing a VPN

Virtual Private Networks (VPNs) are typically deployed in corporate settings in an effort to bolster cybersecurity measures. In 2020 and 2021, our report found that 44% of employers weren't requiring their staff to utilize this security measure. This number ticked up slightly, finding that 46% of employers do not require employees to use VPNs.

In our survey, we asked those who were responsible for information technology at corporations to indicate whether or not they used a VPN. In 2021, nearly 68% of respondents indicated that they used a VPN, up nearly 18% from our 2020 findings. However, in 2022, only 62% of those surveyed indicated that they use a VPN. Respondents who indicated that they do not use a VPN totaled to 34%, and only 3% were unaware of what a VPN is or how it works.

Multi Factor Authentication Utilization Grows

In our 2020 'Password Hygiene and Habits' report, only 16.5% of respondents indicated that they utilized multi-factor authentication at both home and work. In 2021, we saw this number grow to 69.47%.. That said, in 2022, 2021's findings showed significant increases as compared to years passed with nearly 71% of respondents indicating that they use multi-factor authentication at both work and home.



THE CONCEPT OF PHISHING

Phishing is the practice of pretending to be a credible company or individual and sending fraudulent e-mails on their behalf. These emails often include malicious attachments that contain various forms of malware, including ransomware, or links that trick victims into shelling out personal information.

In 2021, nearly 75% of respondents had seen a phishing email. This is a bit higher than we saw in our 2022 results, with 73% of respondents indicating that they had seen a phishing e-mail. 13% of respondents indicated that they did not know what phishing emails were, leaving 14% of individuals who have not seen a phishing e-mail.

Introducing Personal Threats into the Workplace

Reading personal emails at work is a very bad practice because cyber criminals exploit emails to distribute phishing attacks. This creates worry for employers because now they not only have to worry about phishing emails getting in through corporate emails, they have to worry about what's coming in via personal email accounts.

In our 2021 survey, 52% of respondents indicated that they read personal emails at work. However, in our 2022 survey, we saw a decrease of 13-points year over year, with 38% of respondents indicating that they read their personal emails at work.

We also looked into whether or not IT professionals are reading their personal emails at work. One would think they'd know better, but our report found that 52% of IT professionals read their personal emails at work. This is up by 3% since 2021. An additional 14% of these individuals responded that they read their personal emails on their work devices "on occasion."

POOR SECURITY IS SPILLING INTO THE WORKPLACE

How does all this impact business? There are five key factors.

1. **First, it is imperative to change your passwords.** With our survey finding that more than 20% of respondents aren't sure when they last changed their personal email passwords, or haven't changed them at all, general password hygiene is top of mind. Moreover, considering that nearly 21% of employers don't require their employees to change their passwords regularly, it's important to remember that general password hygiene first starts with changing passwords frequently, and making sure they're complex passwords.

2. **Second, rather than just changing your passwords frequently, it is imperative that individuals don't use the same passwords at work and home.** Our survey found that nearly 40% of respondents utilize the same passwords for their home and personal accounts. This is important to note because that's up from 25% in our 2021 survey.

3. **Third, while we see signs of improvement, there's still a significant number of employers who aren't requiring their employees to take additional measures to protect corporate networks.** Of which, as confirmed by the study, 34% of respondents do not utilize a VPN at work. Even more so, 17% of those surveyed indicated that they do not utilize multi-factor authentication at their work.

4. **Fourth, email security.** 100% of respondents had more than one email address in our 2022 survey. Considering this, over half of respondents have admitted to checking their personal emails on work devices. This is important because not only are the individuals opening up external accounts that might expose the network to exploitation, but they are likely checking more than one account. The increased frequency and number of email addresses increases the likelihood of a malicious infection infiltrating a company's networks.

5. **Fifth, phishing threats.** Nearly 12% of respondents indicated that they don't know what a phishing email is. This is important because if employees don't know what something is, they don't know how to spot it. And, considering that phishing emails are carried out through e-mail accounts, the risk only continues to increase as employees check both their personal and professional email accounts throughout the day.

RECOMMENDATIONS

The importance of passwords shouldn't be overlooked. Passwords are one of the greatest vulnerabilities facing both individuals and organizational cybersecurity, yet those who prioritize proper password hygiene still remain at concerning levels.

Top Tips for Individual Users

- Change passwords every six months
- Do not reuse the same passwords
- Use complex passwords
- Enable multi-factor authentication
- Utilizing password lockout thresholds on all work and personal computers
- Do not access personal accounts when connected to an employer's networks
- Complete cybersecurity training

Top Tips for Employers

- Issue passwords to your employees
- If you can't issue passwords, utilize a password generator that will create new passwords for your employees on a routine basis
- Require employees connect to a VPN prior to engaging in work related tasks
- Default computers to a predetermined password threshold lockout time
- Enable multi-factor authentication for access privileges
- Apply filtering measures to online activity
- Mandate employee cyber security training

Changing passwords and taking advantage of additional security measures are the two key takeaways of this report. It is imperative that at a bare minimum you utilize complex passwords, change them frequently, and take advantage of every additional layer of security that you can.

Cyber criminals grow their attacks in frequency and complexity every day. Proper password hygiene and habits are one way we can work together to combat cybercrime.

CONCLUSION

While password hygiene and habits do continue to improve since we've started conducting our study in 2019, based on the results of our 2022 Passwords Habits and Hygiene Report, they're still quite poor.

Individuals and their personal information are still at risk because they fail to practice proper password hygiene. Most notably, people aren't changing their passwords frequently enough, and individuals still aren't taking advantage of additional layers of security such as multi-factor authentication or VPNs. These important tools, paired with changing your passwords frequently, can greatly improve an individual's cybersecurity.

As it relates to employers, employees continue to put their employers at risk by continuing to check personal emails at work. This exposes their employer to external threats, and when one considers that the vast majority of individuals have more than one personal email account, the threat level grows exponentially.

Aside from employees checking their personal emails at work, employers are also at fault for high levels of vulnerability to cybercriminals. Most employers are still allowing employees to choose their own passwords and are opting out of the option of issuing passwords or mandating the use of a password generator. Many employers are still failing to require employees to use a VPN and multi-factor authentication as additional layers of security.

Additionally, it is important that users, regardless of whether it's for their work or personal devices, should never reuse passwords. Each account should have its own password and when it's time to recycle it, never reuse the same password again. This way should an individual's password become compromised, only one password and account have been compromised, rather than the entire kingdom of accounts.

ABOUT PC MATIC

PC Matic, Inc. was established in 1999 by its current CEO and Founder, Rob Cheng. The American Cybersecurity company with operations based in Sioux City, Iowa, and Myrtle Beach, South Carolina, was established with the sole purpose of creating a better way to diagnose common computer problems.

As cyber security threats began to evolve, company leadership knew a new approach to thwart these attacks was critical. This led to the creation of its award-winning cybersecurity software in 2011. Entirely developed, researched, and supported in the United States, PC Matic features a patented whitelist technology, fileless malware detection, and RDP port protection from brute force attacks. Together, these technologies provide the best security protection for endpoint devices around the globe.

For over 21 years, PC Matic has continued to evolve, making them an innovative provider of cloud-based performance and security solutions for homes, businesses, educational institutions, and government agencies.

PC Matic

Rob Cheng
PC Matic CEO and Founder