CYBERSECURITY BY THE NUMBERS

What data can tell us about cybersecurity attitudes and habits

THIS MONTH'S TOPICS:

Password Report Results

The behaviors related to passwords

Cybersecurity Stats

Data and information

Scam of the Month:

Account Deactivation Scams...

Monthly Cyber News:

Takeaways and Recent News...

The National Cybersecurity Alliance has put out their annual report on cybersecurity attitudes and behaviors. They surveyed over 7,000 participants from India, Germany, the UK, US, Canada, New Zealand, and Australia. Topics included artificial intelligence, passwords, software updates, and more.

In this month's newsletter, we'll go over some important findings which discuss the cybersecurity attitudes and habits from the 2024-2025 report. Then we will suggest actionable steps based on the attitudes and behaviors discovered.

PASSWORD REPORT RESULTS

Many organizations lay out password best practices. These include checking if passwords have been breached, avoiding dictionary words and repetitive or simple patterns, and increasing password length. Below are some of the findings about users real password habits.

Personal Information in Passwords

35%

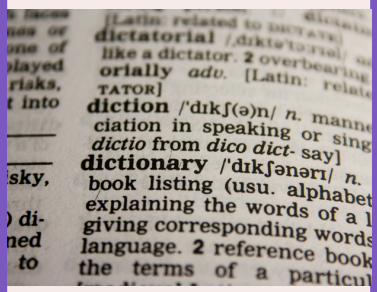
Of all participants surveyed reported using personal information in their passwords.

Password Demographics

Gen Z 52%	**Millennials** 45%
Gen X 28%	**Baby Boomers** 21%

The percent of users who use personal information in passwords by generational group.

Additional Password Stats



40% of participants have created a password using a single dictionary word or a name.

Only 66% of those who have heard of multi-factor authentication (MFA) are actively using it.

65% reported using a separate password either “all of the time” or “a majority of the time.”

Cybersecurity Stats

Data and Information

- **AI Tools and Security**

38% admitted to sharing sensitive work information with artificial intelligence without telling their employer.

- **AI-Generated Content**

44% of employed participants felt confident in recognizing AI-generated content. Though, many noted struggling with the sophistication of phishing messages since the rise of AI.

- **Security Training**

29% of participants reported completing continuous training throughout the year. This means, fewer than 1/3 of people are equipped to stay secure against the newest threats.

- **Multi-factor Authentication**

81% of participants have heard of multi-factor authentication or MFA. This is 11% higher than last year's survey results!

WHAT CAN WE LEARN FROM THIS DATA?

At the end of the report, many key findings were outlined. These include:

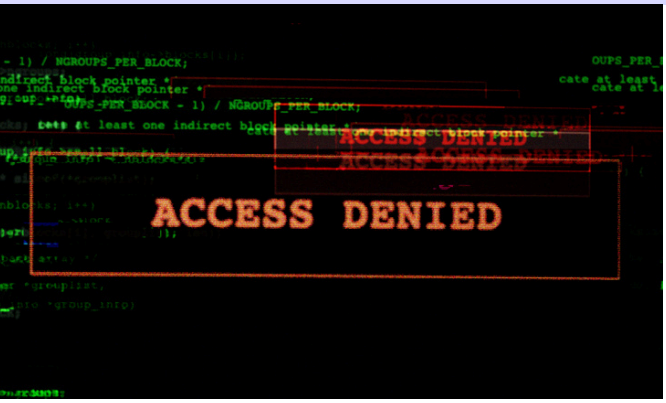
- Just being aware of cybersecurity risks is not enough. We need to make sure we are implementing cybersecurity best practices too.
- Many people are oversharing with AI chatbots. All users should avoid putting sensitive personal or company information into AI chatbot programs.
- Security fatigue is kicking in. Many think it is more difficult to stay safe online.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

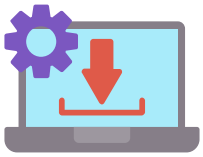
Ava was about to take her lunch break when she noticed an alarming email in her inbox: "Immediate Action Required – Microsoft Account Deactivation." The email claimed that her Microsoft account, where she stored all her project files, would be deactivated within 24 hours unless she called the provided number to resolve a billing issue. Ava quickly dialed the number. A professional-sounding agent answered, reassuring her that the issue could be easily fixed if she provided new billing information and verified her identity by downloading a security patch. She followed his instructions without thinking twice.

The agent then told her to install a remote administration tool so he could assist her further. Though Ava was hesitant, the agent reminded her of the urgency of the situation, and she complied. Within seconds, her computer screen went blank. The scammer had taken control of her device.



Did you spot the red flags?

- Ava should have verified the phone number in the initial email by looking up Microsoft's customer support details.
- If Ava had antivirus software, it may have detected the malicious activity and blocked further access.



Scammers try to trick users into installing software that gives them control over the user's device. Avoid downloading any files or tools unless you are sure they are from a trusted source.

Phishing emails often create a sense of urgency to pressure you into acting without thinking. Always verify account-related issues directly by logging into your account or contacting official customer support channels.

CYBER NEWS

DECEMBER 2024

DATA TAKEAWAYS

One takeaway from this year's collected data is that security fatigue is common. With all of the constant threats and changes, cybersecurity can feel overwhelming. Be sure to take your security one step at a time. Always follow any organizational requirements, and then begin implementing other security best practices into your personal life, as well. Invest in tools that will save you time and effort like password managers, using biometric verification when possible, and engaging in efficiency training.

Visit https://staysafeonline.org/ if you would like to view the National Cybersecurity Alliance's full 139-page report.

MALVERTISING SCAMS ON THE RISE

Many malicious advertising campaigns have recently been discovered. Malvertising occurs when cybercriminals use ads to deliver malware or steal information. Some cybercriminals deploy malware through ads sent via email or social media. Others are using fake CAPTCHA pages to get a user to "verify they are a human" after clicking on an advertisement. Often times malware is delivered without the user knowing. Users should always watch for signs of malware such as an increase in pop-ups on their device or unusually slow device performance.