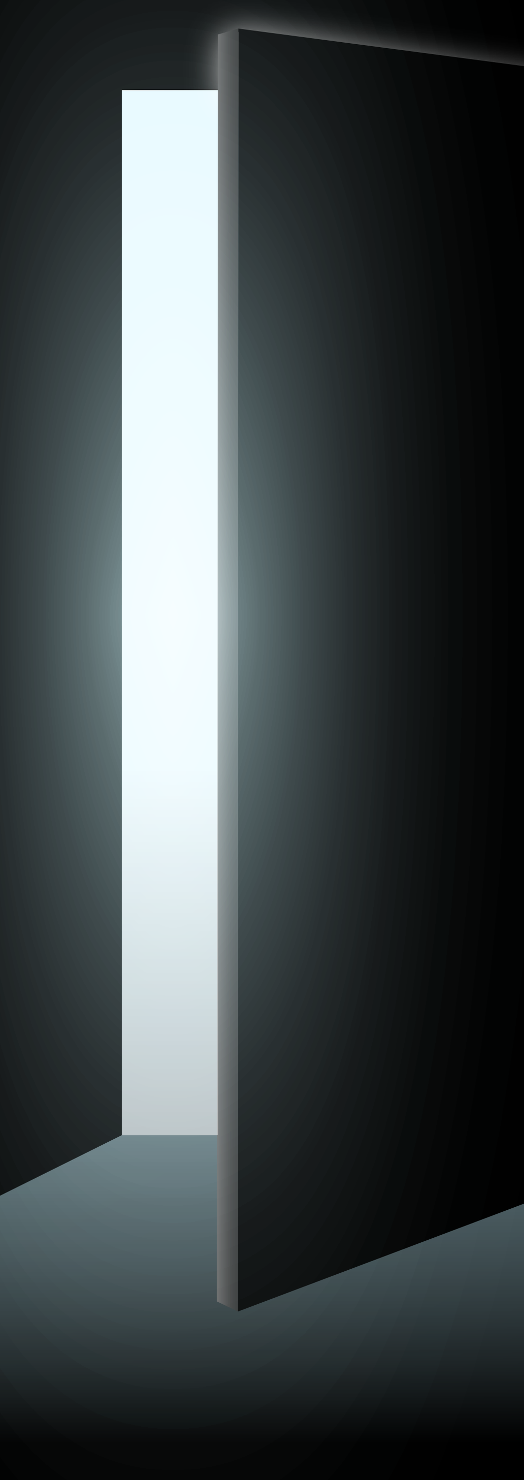
We've seen the data on how they're getting in.



Key insights from the Verizon 2024 Data Breach Investigations Report

Last year was big for cybercriminals. As the Verizon 2024 Data Breach Investigations Report explains, we saw a record-high number of breaches—more than 10,000—with victims spanning 94 countries. We've tracked and analyzed that activity, documenting the trends in attack patterns and arming you with information designed to help you in the ever-shifting cyber threat landscape. Here's some of what we learned.

Vulnerabilities are showing.

180%

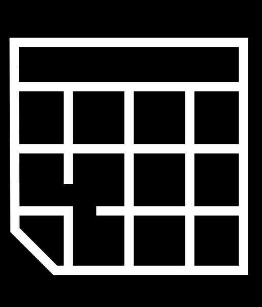
0% 100% 200%

Exploitation of vulnerabilities as an initial access step for a breach grew by 180%—almost triple that of last year—fueled in part by the MOVEit vulnerability and several other zero-day exploits used by ransomware actors.

Defenders must respond faster.

It can take around 55 days for organizations to remediate 50% of critical vulnerabilities after their patches are available—a dangerous lag.

55 days



More training is needed.

68%

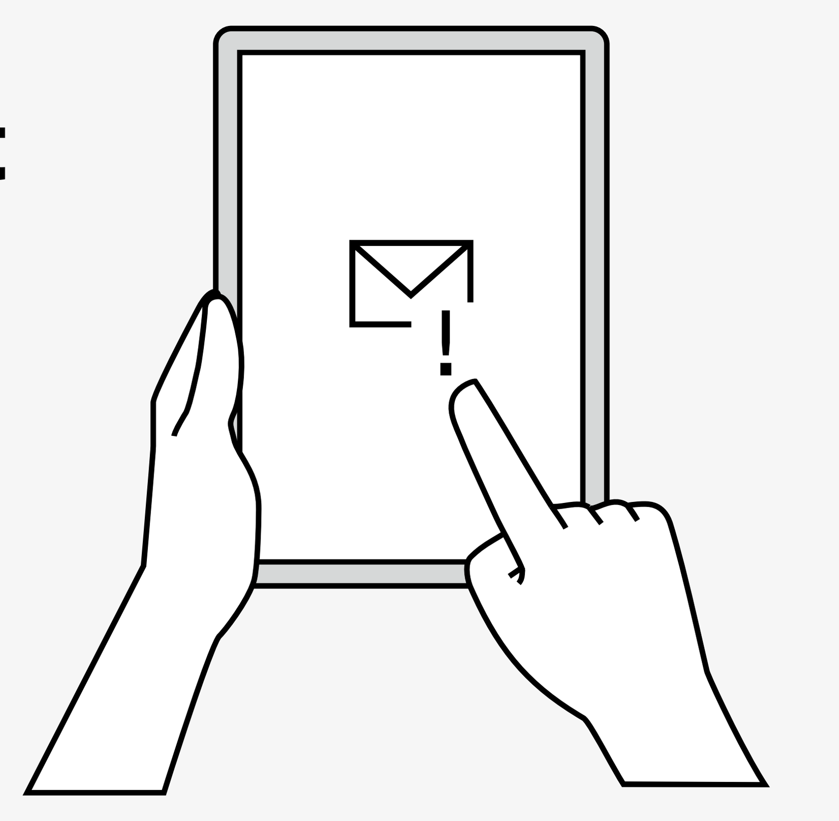
0% 20% 40% 60% 80% 100%

68% of all breaches involved a non-malicious human element, caused by a person who either fell victim to a Social Engineering attack or made some type of Error.

Falling for Phishing—fast

< 60 sec.

The median time for users to fall for phishing emails is less than 60 seconds.



Stolen credentials remain massively popular.

31% of all breaches over the past 10 years have involved the Use of stolen credentials.

31%

0% 20% 40% 60% 80% 100%

Choose your third parties wisely.

15%

0% 20% 40% 60% 80% 100%

15% of breaches involved a third party—including data custodians or hosting partner infrastructures being breached, and direct or indirect software supply chain issues.

"Nice data. It'd be a real shame if anything happened to it."

32% of breaches in 2023 involved some type of Extortion technique, including Ransomware.

32%

0% 20% 40% 60% 80% 100%

$46,000

The median loss associated with financially motivated incidents involving Ransomware or Extortion of some kind was $46,000.[1]

Being compromised is costly.

$50,000

The median loss attributed to Business Email Compromise in 2022 and 2023 was around $50,000.[1]

The cyber threat landscape has only become more complex and dangerous.

Help safeguard your organization by better understanding the current trends and emerging techniques bad actors employ. Read the comprehensive discussion in the complete Verizon 2024 Data Breach Investigations Report—the authoritative source of cybersecurity breach information.

And reach out to your Verizon representative to find out how our experienced team can help support your organization's efforts in the ongoing fight against cyberattacks.

Read the report at verizon.com/dbir.

verizon business

1. Based on data from the FBI's Internet Crime Complaint Center