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

Key insights from the Verizon 2024 Data Breach Investigations Report

Vulnerabilities are showing.

- 180% increase in the median time for users to fall for phishing emails, now less than 60 seconds.
- 68% of breaches involved non-malicious human elements, caused by social engineering or errors.
- 32% of breaches involved third parties, including data custodians, software supply chain issues, and infrastructure breaches.

Defenders must respond faster.

- The median time for users to remediate 50% of critical vulnerabilities after patches are available is 55 days.
- More training is needed to combat this trend.

Falling for Phishing—fast

- Median time for users to fall for phishing emails is less than 60 seconds.
- 31% of breaches involved non-malicious human elements, caused by social engineering or errors.

Stolen credentials remain massively popular.

- 68% of all breaches involved the use of stolen credentials.
- 31% of all breaches involved third parties, including data custodians, software supply chain issues, and infrastructure breaches.

Choose your third parties wisely.

- 15% of breaches involved third parties, including data custodians, software supply chain issues, and infrastructure breaches.

“Nice data. It’d be a real shame if anything happened to it.”

32% of breaches involved third parties, including data custodians, software supply chain issues, and infrastructure breaches.

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

- The median loss associated with financially motivated incidents involving Ransomware or Extortion of some kind was $46,000.¹
- The median loss attributed to Business Email Compromise in 2022 and 2023 was around $50,000.¹

Being compromised is costly.

- 30% of breaches in 2023 involved human error, including mistakes in handling data.
- 32% of breaches involved third parties, including data custodians, software supply chain issues, and infrastructure breaches.

More training is needed.

- 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.

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.

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

© 2024 Verizon. OGINF3980524