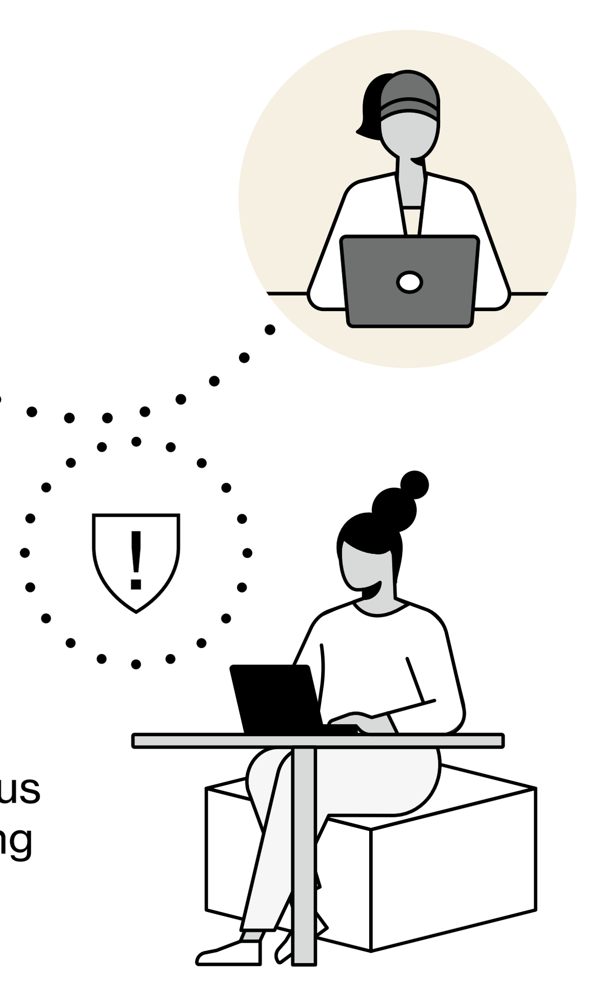
Stack your cybersecurity knowledge—and watch attacks topple

Key findings from Verizon's 2025 Data Breach Investigations Report

It's time to shine a light on shadow actors. In the 2025 Data Breach Investigations Report (DBIR), we decoded 12,195 data breaches across 139 countries. Here's a snapshot of our most critical findings.

Unwitting partner in crime?



15% → 30%

The percentage of breaches where a third party was involved doubled from the previous year, highlighting the importance of choosing partners and suppliers carefully.

Developing a unified cybersecurity posture with partners and suppliers can help reduce vulnerability.

Do you know where your weaknesses are? The bad guys do.

34% ↑

Exploitation of vulnerabilities as an initial access step for a data breach grew by 34%, now accounting for 20% of breaches.

Criminals hope you will respond slowly—or stall out entirely.

32 days

Our analysis shows only about 54% of perimeter device vulnerabilities were fully remediated, and it took a median of 32 days to do so.

More organizations are being held hostage.

44%

of cybersecurity breaches involved ransomware, up 37% from the previous year.

"Pay up or else."

$115,000

Ransomware attacks can take a costly toll on organizations. The median amount paid to ransomware groups was $115,000.

But there's good news, too. The majority of victim organizations – 64% – did not pay the ransoms.

What's the common link in most data breaches? The human element.

60%

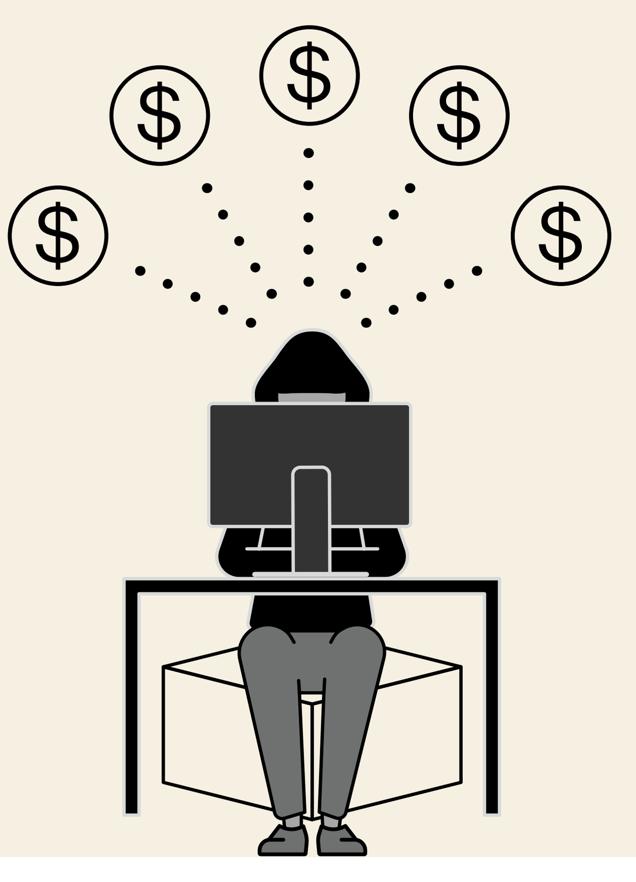
Human involvement in cybersecurity breaches remained about the same as the previous year – 60%.

Credential abuse and social actions – like phishing – were major factors in these types of breaches.

State eyes are on the dollar signs.

28%

Espionage-motivated attacks now account for 17% of security breaches. But espionage isn't the only thing state-sponsored actors were involved in – roughly 28% of state-sponsored incidents had a financial motive.



No device is off-limits.

30% managed devices

46% non-managed devices

Our analysis of infostealer credential logs found that 30% of compromised systems were enterprise-licensed devices. However, 46% of the systems with corporate logins in their compromised data were non-managed – in other words, they were personal devices.

The bots are in on it, too.

2x

Data shows that threat actors are powering their cyberattacks with AI. Synthetically generated text in malicious emails has doubled over the past two years.

Do you know what your employees are sharing with AI?

15%

of employees routinely accessed generative AI platforms on their corporate devices – increasing the potential for data leaks.

You need the most comprehensive and trusted cybersecurity breach report on your side: DBIR.

When you know the tactics hackers use to exploit organizations, you can better protect your own systems. Take the first step in helping to strengthen your security posture by reading the 2025 Data Breach Investigations Report.

Reach out to your Verizon representative to learn how our experienced team can help you navigate the ever-changing threat landscape. Together, we can help safeguard your data from the shadows.

Read the report at verizon.com/dbir.

verizon business