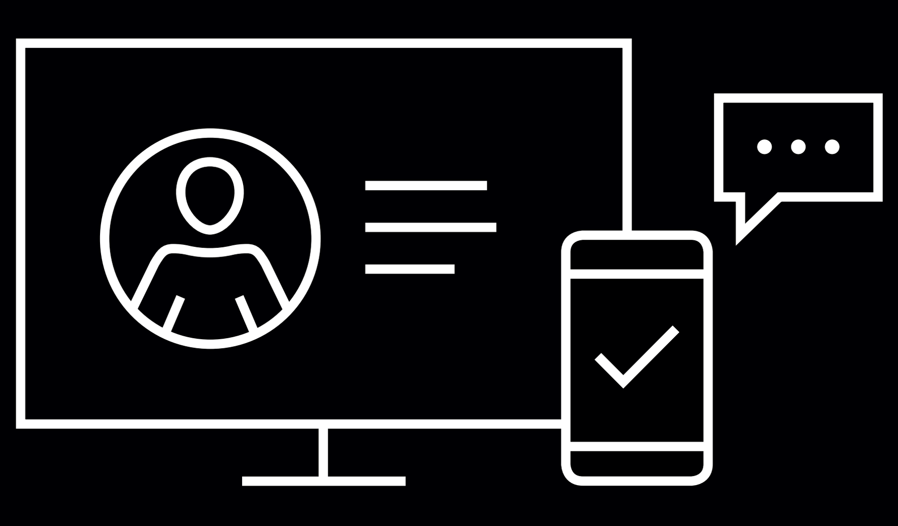
Comprehensive. Authoritative. Trusted.

Seven key insights from the 2023 Verizon Data Breach Investigations Report

Cybercriminals are coming for data, and they're using more types of attacks against organizations like yours.

That's the unmistakable takeaway from our 2023 Data Breach Investigations Report, which catalogs and analyzes the past year's trends in cybercrime. With deep insight and distinctive humor, it explores the most common, most dangerous and fastest-growing attack patterns wielded against organizations worldwide.



Pretexting rose.

50%

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

50% of all Social Engineering incidents in 2022 used pretexting—an invented scenario that tricks someone into giving up information or committing an act that may result in a breach.

"We have your data. Pay us."

24% of all breaches involved ransomware—maliciously encrypting data and demanding a ransom to return or unlock it. It's present in more than 62% of all incidents committed by Organized crime actors and in 59% of all incidents with a Financial motivation.

24%

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

Threats are accelerating.

>32%

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

More than 32% of all Log4j vulnerability scanning—exploiting a flaw in this ubiquitous Java-based utility that can give control of your servers to hackers—occurred in the first 30 days after release.

This shows how quickly threats can go from proof of concept to mass exploitation.

Most threats come from outside the organization. But insiders are dangerous, too.

83%

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

83% of breaches involved external actors, primarily from Organized crime groups with Financial motives.

19%

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

19% involved internal actors, who caused both intentional and unintentional harm through Misuse and simple human errors.

Help people-proof your systems.

74% of all breaches include the human element through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

74%

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

The bad guys are clever, persistent and, too often, successful.

49%

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

49% of breaches by external actors involved Use of stolen credentials, while Phishing made up 12% of external attacks. Attackers used the Exploit vulnerability technique in 5% of breaches.

This shows the importance of anticipating diverse attack vectors.

And—surprising no one at all—it's (almost) always about the money.

95% of breaches are financially driven.

95%

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

Protecting your organization starts with understanding the threats you face. Reducing the mean time to detect a breach can make all the difference in how effectively your organization recovers from one.

Read the complete Verizon 2023 Data Breach Investigations Report for the whole picture. Then speak with your local Verizon Business representative to learn how Verizon can help harden your infrastructure against cyberattack.

Read the report at verizon.com/dbir.

verizon