Phishing kits with high breakthrough rates: what security teams should know



Push Security tracks a 'breakthrough rate' for phishing kits: the share of attacks that evade email security, web gateways and safe browsing and reach the user. Some kits do this far more often than others.

- Every phishing attack must pass email security, web filtering and safe browsing before reaching an employee.
- Push Security defines breakthrough rate as the share of attacks that get past those layers and reach the user.
- Some phishing kits succeed at this far more often than others.
- Security teams are advised to focus on the kits that break through most often.

A new piece from Push Security looks at phishing through a practical lens: not how many attacks are sent, but how many actually get through the controls an organisation has put in place.

The metric

The vendor uses the term **breakthrough rate** for the share of attacks that get past email security, web gateways and safe browsing and reach the user. The premise is simple: every phishing attack has to clear these layers first, and some kits clear them much more often than others.

The excerpt we reviewed does not list the kits, techniques or rates, so we do not repeat any here. The full article should be read directly before drawing conclusions about specific tooling.

Why it matters

For a regulated institution, the useful takeaway is about prioritisation. Awareness content, detection rules and response playbooks should be shaped by the kits and techniques that actually reach employees, rather than by the overall volume of phishing reports.

It also reinforces that perimeter email and web controls are one layer, not a guarantee. What happens after a message lands, such as user reporting, identity protections and rapid response, deserves equal attention.

Suggested approach

Review the source material, compare it with your own phishing telemetry, and decide whether your testing reflects the kits that are most likely to bypass your stack.

What to do now

1. Read the full Push Security article and note any kits or techniques relevant to your environment.
2. Compare its themes with your own phishing telemetry and user reports to find what reaches inboxes.
3. Run phishing simulations that reflect evasive techniques, not only basic lures.
4. Confirm users have a simple reporting route and that the SOC triages reports quickly.
5. Review identity protections so a successful phish does not lead directly to account takeover.