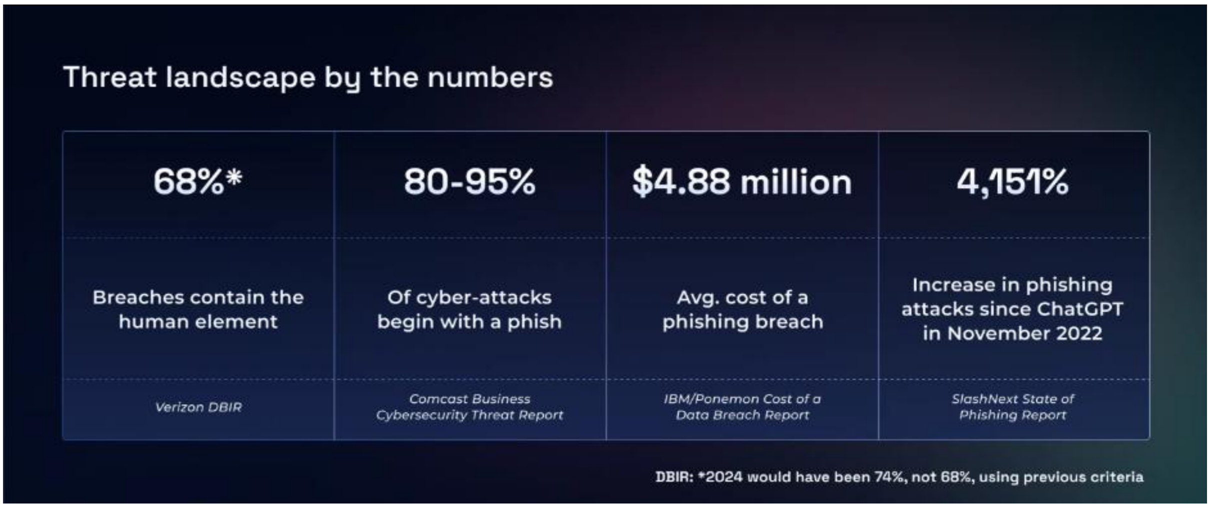
Phishing Attack Playbook

Introduction

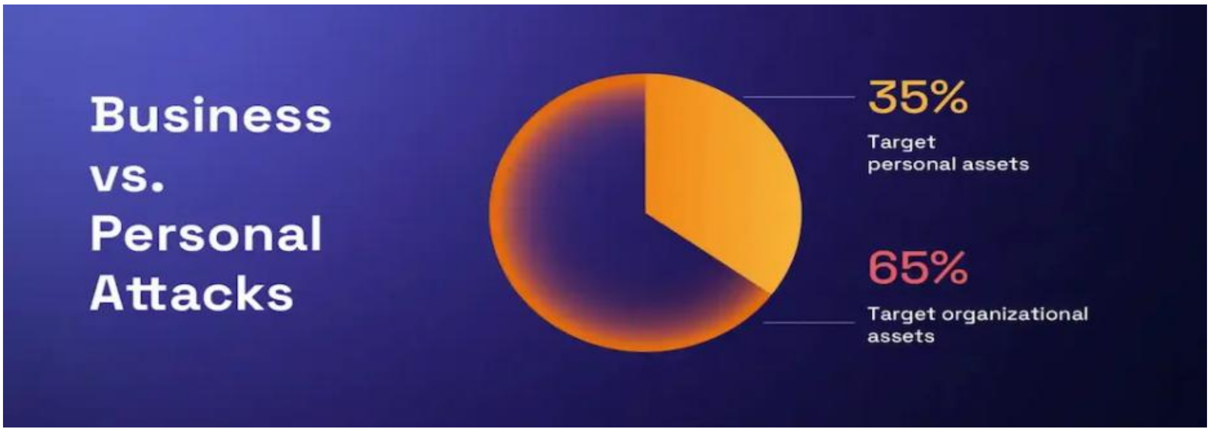
Phishing is still the most common way attackers get in. It mixes technical tricks with social manipulation, so your response has to cover both technology and people. This playbook lays out how to detect, validate, respond, and learn from phishing incidents in a way that teams can actually follow. Below are the statistics provided by Hoxhunt

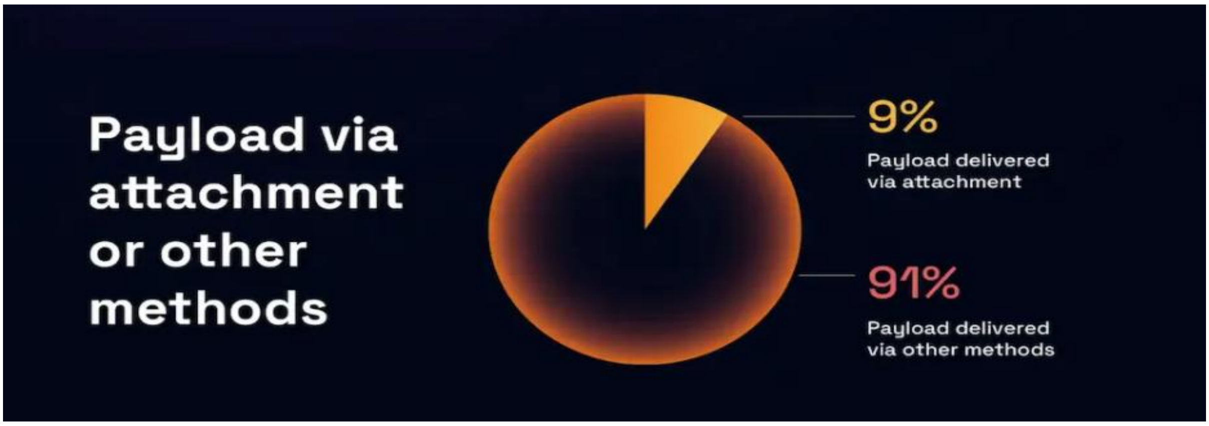


Threat landscape by the numbers

68%*	80-95%	$4.88 million	4,151%
Breaches contain the human element	Of cyber-attacks begin with a phish	Avg. cost of a phishing breach	Increase in phishing attacks since ChatGPT in November 2022
Verizon DBIR	*Comcast Business Cybersecurity Threat Report*	*IBM/Ponemon Cost of a Data Breach Report*	*SlashNext State of Phishing Report*

DBIR: *2024 would have been 74%, not 68%, using previous criteria





Detection Methods

Watch these sources for signs of phishing:

- Alerts from email security gateways that flag suspicious messages
- Reports from employees using your phishing report channel or button
- Security tools that notice unusual link clicks or unexpected file downloads
- Strange authentication events right after a suspected phishing email was delivered
- Signs of unexpected data access or credential misuse

When multiple people report similar messages, treat that as a possible campaign. Correlate reports across mail systems, identity logs, and endpoint telemetry so you can spot coordinated attempts quickly.

Validation and Analysis

Once an email is flagged, validate it safely and quickly:

- Open and analyse suspicious messages only in an isolated environment or sandbox
- Extract and inspect URLs without clicking them directly. Use URL decoders and safe browsing tools to see where they lead
- Run attachments in sandbox environments and review the results for malicious activity
- Check who was targeted. Was it a single person, a specific department, or many users across the company?
- Determine what data could be at risk if users followed the malicious link or opened the attachment
- Search mail servers and inboxes for similar messages to understand how widespread the campaign is

The goal in this stage is to confirm whether this is a one-off phishing attempt, a broader campaign, or a targeted spear phishing attack. That determines the scale of your response.

Response Actions

Respond in a way that matches the scale and severity of the threat:

- Block sender domains and known malicious URLs at your email gateway and edge firewall immediately when they are confirmed malicious
- Run a company wide search for similar messages and apply automated quarantine or removal where your mail system supports it
- Force password resets for accounts that likely had credentials exposed or that show signs of compromise

- Enable or enforce additional authentication steps for affected users, such as multi factor authentication or step up verification where possible
- Scan endpoints that accessed suspicious links or files to look for indicators of compromise
- Review network logs and DNS requests to find any post compromise activity such as command and control traffic or data exfiltration attempts

Make sure these actions are documented and that changes are communicated to IT and affected teams. Fast containment keeps the incident small.

User Management and Education

People are both the target and the strongest defense. Include these human focused steps:

- Use prewritten communication templates to quickly notify the organization about active phishing campaigns without causing panic
- Provide clear instructions to users who may have clicked links or entered credentials, including how to reset passwords and who to contact for help
- Run targeted training for departments that are frequently targeted or were specifically hit by this campaign
- Track metrics such as number of reports, click rates in simulated phishing, and time to remediation to measure awareness and program effectiveness

Make your communications short, direct, and actionable. People respond better to instructions they can follow immediately.

Post Incident Work

After the incident is contained, do the follow up:

- Preserve evidence from mail systems, endpoints, and network logs in case legal or regulatory action is needed
- Conduct a root cause analysis to find how the message bypassed controls and what user behaviors helped the attack succeed
- Review and patch gaps in email filtering, web proxy rules, and endpoint protection that the attack exploited
- Update response playbooks with lessons learned and make those changes available to the team
- Schedule refresher training or targeted campaigns to address the specific tactics used by the attackers

Document everything. Good documentation is how you improve and reduce repeat incidents.

Quick Practical Tips

- Encourage people to report suspicious messages rather than delete or forward them
- Keep a short incident checklist so analysts can act fast under pressure
- Maintain a blocklist of malicious domains and a whitelist of known good vendors to speed up filtering decisions
- Use safe tools for URL and attachment analysis so analysts do not expose internal systems