2025-05-22 Summary Phishing Data Breach

Incident Type: Phishing / Data Breach Attempt
Date: 2025-05-22
Reported by: Astor Mydz – Finance Department
Investigated by: Luis Gutierrez – SOC Team
Current Status: Resolved
Severity: Critical

- User received a phishing email from `Malicious@Domain.com`.
- The phishing attempt aimed to exfiltrate banking credentials.
- Multiple high-level transaction alerts triggered simultaneously, signaling possible compromise.
- Immediate mitigation included isolating the affected systems and resetting all users' passwords.

Timeline of Events

Time (UTC)	Event Description	Action Taken
08:16	User reported receiving a suspicious phishing email.	Alert sent to SOC Team.
08:18	The SIEM generated multiple alerts of high-level transaction attempts.	Assigned analyst to investigate.
08:20	Malicious domain identified: `malicious-domain.com`.	Domain blocked in firewall.
08:22	Review of affected accounts and potential credential exposure.	No credentials compromised (all passwords reset immediately).
08:25	Containment and mitigation actions completed.	Passwords reset for all affected users.
08:30	Incident verification completed.	Case closed.

Indicators of Compromise (IoCs):

- Phishing domain: `malicious-domain.com`
- Suspicious IP: `192.xxx.x.xx`
- File hash: `d41d8cd98f00b204e9800998ecf8427e`

Final Thoughts:
Even though the case was resolved quickly, we must raise awareness among employees to prevent a greater tragedy.

How:

- Conduct phishing simulations more frequently
- Stay informed about new threats and technologies
- Hold regular meetings to discuss phishing and security topics