acceligence

You clicked the link. Now what? A director's playbook for recovering from a phishing attack

Insight

November 18, 2025

Category: cybersecurity

Tags: board of directors, breach, hacked, hacker, password, phishing, smishing

Every director's worst nightmare: *you clicked it.*

The email looked legitimate – maybe a message from your bank, a vendor, or your CEO asking for quick action. It had all the right logos, the right tone, even the right signature. But when you clicked the link or opened the attachment, something didn't feel right. Maybe the page looked slightly off, or the request seemed out of character. Then it hits you: this might have been a phishing attempt.

What happens next will determine whether it's a harmless scare or a major security incident. The truth is, even the most experienced leaders fall for phishing attacks – they're engineered for people like you: busy, decisive, and trusting of what looks official. The key isn't to avoid every risk; it's to respond intelligently when something slips through.

This step-by-step playbook is your calm, practical guide for what to do next. No technical jargon, no shame – just a clear path from panic to recovery.

Step 1: Don't panic, but don't wait

The moment you realize what happened, your first reaction might be embarrassment — or worse, denial. "It probably wasn't real." "I'll just delete it." "No one needs to know." Those few minutes of hesitation can make the difference between containment and crisis.

Take a deep breath. Then act decisively.

Director's tip: Your speed matters more than your technical skill. Think "call 911," not "learn first aid."

If you're on a corporate laptop, disconnect from Wi-Fi immediately. Don't try to "fix it" yourself — don't restart, delete, or scan. Just isolate the device and call for help. If it's a personal device used for company email or logins, do the same: get it off the network. Your IT or security team can't protect what they don't know about, and they'd always rather respond to a false alarm than an undetected breach.

Resource spotlight: CISA's phishing guide offers quick steps for identifying and reporting phishing attempts – a solid reference to share with your team.

Step 2: Notify your security team immediately

You might worry about "bothering" the security team or looking careless. Don't. Cybersecurity professionals handle phishing incidents daily; your honesty gives them the head start they need to protect the company.

Call or message your CISO, IT director, or managed security provider right away. Use a separate device if the one you have is compromised. Tell them exactly what happened: when you clicked, what the email or text message said, and whether you entered any credentials or downloaded files. If your device is still on and useable, they may ask you to forward the original message (without replying to it). The more context they have, the faster and more effectively they can respond.

From there, they'll likely block the sender, scan for related threats, and monitor your accounts for unusual activity. The key word here is containment. Quick, transparent communication enables that – silence does not.

Remember: Reporting an incident early is an act of leadership, not failure. You're protecting your organization's time, money, and reputation.

Step 3: If you entered credentials, change them immediately

If you entered a username or password into a suspicious site, assume that information is compromised. Attackers often move quickly, testing stolen credentials within minutes.

Change your passwords immediately – starting with your email and any accounts linked through single sign-on (SSO). Use a new, strong password that's unique to that account. If possible, have your IT team revoke any active sessions, credentials, or access tokens/certificates.

And if your organization hasn't already, now's the time to enable multi-factor authentication (MFA). Even if your

credentials were stolen, MFA can stop attackers from gaining entry.

Director’s tip: MFA is one of the simplest, most cost-effective protections available. If you’re unsure whether it’s enforced across all critical systems, make it a board-level question.

Resource spotlight: NIST Digital Identity Guidelines explain modern best practices for authentication and password management.

Step 4: Don’t delete the evidence

Your instinct may be to delete the phishing email or browser tab immediately – a kind of digital “clean up.” Don’t. That email is now a key piece of evidence for your security team. It contains metadata and forensic clues that can help identify who sent it, how it bypassed filters, and whether anyone else received it.

Avoid running any software or antivirus tools unless directed. Don’t forward the message to colleagues (you don’t want them clicking too). Simply leave it untouched and isolated.

If your device is compromised, your security team might make a forensic copy to analyze what the attacker did. It’s not about blame – it’s about understanding exposure and protecting others.

Remember: Every incident is data. Preserving that data helps your organization strengthen its defenses.

Step 5: Stay ahead of the communication curve

Phishing incidents involving executives can have reputational ripple effects. If sensitive data, credentials, or correspondence could have been accessed, communication needs to be deliberate and transparent.

Your CISO or communications lead will coordinate next steps – possibly including notifying regulators, vendors, or even customers, depending on what systems were affected. Your role is to ensure the company responds quickly, clearly, and credibly.

Want to be proactive? Ask your team:

•Who should I call?
•Who needs to be informed?

•What's the timeline?
•What's our message?

Transparency builds confidence. Evasion destroys it.

Director's tip: When in doubt, overcommunicate with your security and legal leads – and under-communicate externally until facts are verified.

Step 6: Review your exposure with experts

Once the immediate response is under control, request a full technical and governance-level assessment. This should include digital forensics, system monitoring, and a review of what was potentially accessed or exfiltrated.

Your IT or security provider should produce a timeline: when the attack occurred, how it was detected, and what actions were taken. Ask for plain-English explanations – no acronyms, no firehose of technical terms. As a director, your focus should be on impact and mitigation, not code-level details.

If you sit on multiple boards, make sure this review also informs your oversight in other organizations. Attackers frequently reuse tactics and stolen information across industries.

Resource spotlight: The SANS Incident Handler's Handbook outlines best practices for managing and documenting security incidents. Most organizations have a version tailored for themselves and some even create versions for the board.

Step 7: Turn the incident into institutional learning

A phishing incident can feel personal – but it's really organizational. Every successful phish reveals gaps: in technology, awareness, or process. The most resilient companies use those gaps as fuel for improvement.

Encourage your CISO or risk officer to conduct a post-incident review and share findings with the board. What worked? What failed? How will detection, response, or training evolve? This isn't about assigning blame; it's about building collective muscle memory.

Many boards run tabletop exercises – simulated crisis scenarios – using real incidents as case studies. They're not just valuable for management teams; they help directors practice asking the right questions under pressure.

Director's tip: Ask your CISO to present three key takeaways from every incident – one technical, one procedural, and one cultural. That ensures learning spans the entire organization.

Step 8: Strengthen your personal defenses

Executives are prime phishing targets because they have access, authority, and predictable patterns. Attackers know directors approve transactions, sign documents, and hold sensitive communications. Strengthening your own habits is the simplest way to reduce risk company-wide.

Be skeptical of any email that creates urgency or asks for credentials, even if it looks legitimate. Hover over links before clicking to confirm the actual domain. When in doubt, verify through another channel – call, text, or message the sender directly.

Remember: The goal isn't paranoia – it's posture. Security awareness is the new executive fitness.

Use a password manager to store unique, complex passwords for each account, and enable MFA wherever possible. Keep your devices updated, and avoid using personal email or social media to discuss company matters. Also, freeze your credit with all the credit bureaus, sign up for monitoring for you and your family, and consider subscribing to personal digital threat protection like Reputation Defender.

Resource spotlight: The National Cybersecurity Alliance's Stay Safe Online resource hub provides practical guidance for executives and families alike.

Step 9: Close the loop with the board

Once the situation is resolved, take the time to close the loop formally. Your CISO should document the timeline of events, actions taken, and lessons learned. This should be presented in a board or committee meeting – not buried in a technical report.

Request a brief written summary from your CISO or risk lead outlining:

•The nature of the incident
•Response measures and timelines
•Impact assessment (what, if anything, was compromised)
•Policy or control changes made since

Boards that treat these reports seriously build trust with regulators, investors, and employees alike. It signals that

cybersecurity isn't a side issue – it's core to governance and resilience.

Director's tip: Ask for a brief update six months later to verify that any promised improvements were implemented and are effective.

Step 10: Move forward, smarter

Everyone clicks eventually. The phishing landscape evolves faster than any individual can keep up with. What defines you as a leader isn't immunity – it's composure, transparency, and the discipline to learn quickly.

Recovering from a phishing attack isn't just about incident response; it's about leadership maturity. You're modeling calm under pressure, collaboration over blame, and clarity over confusion. Those are the same qualities that drive effective governance in any crisis.

Remember: Cyber resilience isn't perfection — it's preparation, practiced over time.

So the next time an email makes you pause – good. That pause is awareness. And the fact that you now have a playbook means that even if something slips through again, it won't derail your confidence or your company.

Final thought

Phishing isn't just an IT problem. It's a human one – and humans, fortunately, can learn. Every click, every scare, every recovery builds organizational wisdom. The more directors treat these moments as opportunities for clarity instead of shame, the safer the entire enterprise becomes.

When you clicked, it felt like a mistake. But handled well, it can become a masterclass in crisis leadership – one that strengthens not just your systems, but your example.