Cybersecurity Basics

ComplyClinic Playbook

# Someone Clicked the Link: Phishing Response Playbook

A calm, step-by-step guide for containing a phishing incident before it becomes a larger breach.

**Audience:** Any organization that needs a practical first-hour response when a user clicks a suspicious link.

General educational resource only. This is not legal advice, certification advice, or a substitute for a formal security risk analysis, CMMC assessment, or incident response engagement.

## First rule: do not panic

A fast, calm response matters more than blame. Many incidents become worse because employees hide the mistake or leadership waits too long to investigate.

Create a reporting culture where staff can say, I clicked something, without fear.

## First 15 minutes

Disconnect the affected device from the network if malware is suspected. If it was only a credential phishing link, focus on account containment first.

Capture the email, link, sender, time clicked, account involved, and any login prompts or files downloaded.

## Contain the account

Reset the password, revoke active sessions, verify MFA settings, check recovery email and phone numbers, and review recent sign-ins.

Look for mailbox forwarding rules, inbox rules that hide messages, suspicious OAuth app grants, and unusual sent mail.

## Check for business impact

Determine whether invoices, payroll, banking, patient data, customer records, or vendor payment instructions were accessed or changed.

If money movement or regulated data may be involved, escalate immediately to leadership, counsel, cyber insurance, or incident response support.

## Communicate carefully

Do not overstate or understate. Document known facts, unknowns, containment actions, and next steps.

If customers, patients, vendors, or partners may be affected, coordinate communications before sending broad notifications.

## Prevent recurrence

Enable MFA, improve spam and phishing filtering, block malicious URLs, run targeted training, and add procedures for payment change verification.

Use the incident as a practical training example, not a punishment event.

## After-action checklist

Document timeline, affected systems, accounts reviewed, data exposure determination, lessons learned, and control improvements completed.

Next step: Need help after a suspected phishing incident? Schedule a consultation and start containment quickly. Schedule now

**Need help turning this into a practical roadmap? Book a free consultation at complyclinic.com.**

ComplyClinic • Practical cybersecurity, compliance readiness, automation, app development, and AI governance support.