Phishing response

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Help desk, IT leads and anyone who administers email.

What to do when a fake email, message or site arrives that is trying to steal credentials or install malware. The goal is to find out who fell for it, cut off the attacker's access and stop the message from circulating further.

Signs it is happening

- An email pressing you to log in, pay or download a file.
- A sender whose domain looks like the legitimate one but is off by one letter.
- A link whose real destination does not match the text it displays.
- Users reporting that they entered their password on a strange page.
- New forwarding rules on a mailbox or logins from another country.

How serious it is

High	Someone entered credentials or opened a malicious attachment; privileged accounts involved.
Medium	A campaign aimed at several users, with no evidence that anyone fell for it.
Low	A generic email reported and blocked before anyone interacted with it.

First hour

- [ ] **1.** Ask the person who reported it not to forward the message; have them send it as an attachment.
- [ ] **2.** Search the mail server to find out how many people received the same message.
- [ ] **3.** Delete the message from every mailbox and block the sender, domain and link.
- [ ] **4.** Find out who clicked and who entered data: review the proxy and mail logs.
- [ ] **5.** Change the password and close the sessions of every person who entered credentials.
- [ ] **6.** Alert the rest of the staff with a screenshot of the message so they can recognize it.

Preparation (before the incident)

- Set up SPF, DKIM and DMARC on your domain, with a reject policy.
- Turn on two-step verification for the email of all staff.
- Provide a button or mailbox for reporting suspicious emails.
- Train staff with real examples at least twice a year.

Detection and Analysis

- Review the full headers: real sender, servers and SPF/DKIM result.
- Analyze links and attachments in an isolated environment, never on your work computer.
- Classify the objective: credential theft, malware or payment fraud.
- Extract the indicators: domains, IP addresses, hashes and subject lines.

Containment

- Block the indicators in email, proxy, DNS and firewall.
- Revoke the sessions and tokens of the compromised accounts.
- Remove forwarding rules and delegations that the mailbox owner does not recognize.
- Isolate the computer of anyone who opened a malicious attachment.

Eradication

- Request the takedown of the fake site from the hosting provider and the domain registrar.
- Report the link to the browsers (Google Safe Browsing, Microsoft SmartScreen).
- Scan with antivirus the computers of those who interacted with the message.

Recovery

- Restore users' access with new passwords and two-step verification turned on.
- Review the activity of the affected accounts for 30 days.
- Confirm that no fraudulent emails were sent from the compromised accounts.

Lessons Learned

- Measure how many received it, how many clicked and how long the first report took.
- Tune the mail filters with what you learned from this campaign.
- Use the case, without singling anyone out, in the next training session.

Evidence to preserve

- The original email in .eml or .msg format, with headers.
- A screenshot of the fake page and its full address.
- Mail and browsing logs of the users involved.
- The list of recipients and of those who interacted.

What not to do

- Forwarding the suspicious email: it spreads the link and strips useful headers.
- Opening links or attachments to “see what they do” on a work computer.
- Blaming whoever fell for it: it discourages the next person from reporting in time.
- Changing the password without closing the open sessions.

Who to notify

- The organization's staff, with the example of the message.
- The impersonated brand, if it is a bank or a vendor.
- Customers, if the fraudulent email was sent from one of the organization's accounts.
- cert.gt, with the indicators, to alert other organizations.

When to close the incident

- The message has been deleted from every mailbox.
- All compromised accounts have a new password and two-step verification.
- The indicators are blocked and the fake site has been reported.
- There is no anomalous activity on the affected accounts.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).