

Phishing response card

For employees: check suspicious messages, report safely and respond promptly after a possible mistake. IT or information security should fill in internal reporting routes before distribution.

Before you click

An unexpected request, urgency, new bank details or a request for credentials? Pause. A familiar sender address and polished wording do not prove authenticity.

Verify through a known contact or an official app you open yourself. Do not use the phone number, reply function or sign-in link in the suspicious message.

Do not open links, attachments or QR destinations to try them out. Never share passwords or MFA codes; reject unexpected MFA prompts.

Report the suspicion internally

Use the approved report button or agreed IT contact. State the time, affected service and actions you took. Preserve or submit the message as instructed internally; do not circulate it to colleagues. Do not engage with the sender.

If you already acted

Situation	What to do now
Opened a link	Stop interacting, enter nothing further and promptly inform IT. A click alone does not prove infection; IT assesses the situation.
Entered a password or approved MFA	Notify IT immediately. Change affected passwords through a known route on a trusted device, including reused passwords. Ask IT to review and revoke active sessions or access as needed.
Opened a file or sent money	Contact IT immediately and follow device instructions. Do not attempt your own cleanup or delete evidence. For payments, also contact finance and the bank using known contact details.

Reporting contact / report button: _____

Backup contact and phone: _____

Internal phishing report

This template supports the handover to IT. Report urgent cases immediately through the agreed route; do not wait until every field is complete.

Field	Your information
Time and your callback contact	
Channel and displayed sender	
Subject or short description	
Affected account or device	
Actions you took and when	
Observed effects or warnings	
Contact already notified and case reference	

Do not enter passwords, MFA codes or complete customer records. Submit original messages and attachments only through the reporting route approved by IT.

Example of a brief report

Fictional example: "09:15, email claiming to be from a supplier asking to change bank details. I read it, opened no links and made no payment. Please review. Reach me through my internal work contact."

Adapt and share

Original Paragamix GmbH template. Free to use internally, adapt and share with clients. Complete and review internal contacts and procedures before use. A source link is welcome but not required.

[NIST Phishing](#) | [BSI CSN response guide \(German\)](#)

[Current version and tools](#)