

CHEAT SHEET · TOMORIS TOOLBOX

Recognizing Phishing: Cheat Sheet for Employees

Warning signs, checking steps, and special forms of phishing, what to do after a click, and how to report correctly in Austria

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/phishing-erkennen-spickzettel

AT A GLANCE

6

Warning signs with an example and a way to check

6

Special forms from CEO fraud to MFA requests

10

Questions to post

10

Sources: BSI, BKA, Watchlist, Microsoft, CISA

WHO IT IS FOR

- All employees who handle email, text messages, chats, and calls, no IT knowledge required
- Managers who share the cheat sheet, post it, or use it in training
- Accounting, purchasing, and assistants who initiate or approve payments
- IT managers who define reporting channels and plan training

WHAT THIS COVERS

Phishing messages often look genuine today: flawless language, a familiar logo, a seemingly trusted sender. This cheat sheet shows the typical warning signs with an example and a way to check each one. It covers special forms, from CEO fraud to QR codes and calls to MFA requests you did not trigger, and what to do immediately after a click. It also includes the reporting channels in Austria and a template for your internal contacts. The guidance is based on BSI, the Austrian Federal Criminal Police Office (Bundeskriminalamt), Watchlist Internet, Microsoft, and CISA.

This cheat sheet provides an overview and does not replace your company's rules. Enter your internal reporting channels in the template before sharing it. Names and functions in Outlook may differ depending on the version and your IT's settings; contact details of the reporting offices as of October 25, 2026.

CONTENTS

01	The Basic Rule: Pause, Check, Report	2
02	Six Warning Signs and How to Check Them	3
03	Check in Six Steps	4
04	Special Forms: CEO Fraud, QR Codes, Text Messages, Calls, MFA	4
05	After a Click: Act Immediately	5
06	Report Correctly: Internally and in Austria	6
07	Checklist to Post	6
08	For Managers and IT: Set the Framework	7
09	Sources	8

01

The Basic Rule: Pause, Check, Report

Phishing comes via email, text message, chat, phone call, or QR code. Flawless language is no all-clear.

Pause

Pressure is the warning sign

Urgent calls to action and threatened consequences are typical features (BSI, Federal Criminal Police Office).

Check

Through another channel

Not via the link or number in the message, but via contact details you look up yourself (BSI).

Report

Including your own click

Also report suspicious emails, links, and attachments you have opened, as early as possible (CISA).

Phishing messages pretend to come from a known person or organization, such as a bank, a parcel service, a public authority, a manager, or the IT department. They aim to get you to open a link, launch an attachment, enter credentials, or transfer money (BSI, CISA). Error-free text is no proof of authenticity: according to the BSI, typos are now only rarely a clear indication. Pay attention to the request, not the language.

02

Six Warning Signs and How to Check Them

Sender, pressure, links, attachments, unusual requests, and requested data: feature, example, and way to check.

Warning signs in email, text messages, and chats (BSI, Federal Criminal Police Office, Watchlist Internet, Microsoft)

FEATURE	EXAMPLE	HOW TO CHECK
Sender does not match	Display name "IT Service," but an unfamiliar address behind it; a domain with extra numbers or altered letters	Hover over the sender line without clicking: a different address may be behind it (BSI). If the signature does not match the address, that is a warning sign (Microsoft).
Pressure and threats	"If you don't do this, we will unfortunately have to block your account ..."	Don't let yourself be pressured (Federal Criminal Police Office). Clarify the matter yourself via the known website or number.
Link leads somewhere else	A "Confirm account" button with a random string of characters, a short link, or an address such as "www.135x-Bank.de" behind it	Hover over the link, or press and hold it on a smartphone: the real destination address appears (Watchlist Internet). "https://" is no all-clear (BSI).
Unexpected attachment	Extension .exe or .scr, a double extension such as .pdf.exe, a request to enable macros	Don't open attachments of suspicious emails (BSI). If a file asks you to enable macros or install something, that is a clear sign (Microsoft).
Unusual request	Management writes from a private address and demands an urgent, confidential transfer	Become suspicious when a known sender makes an unusual request (BSI). Call the person back through a known channel (Watchlist Internet).
Confidential data requested	Password, PIN, TAN, or credit card number by email, text message, form, or phone	Banks and authorities never ask for your password by email (BSI), and bank employees never ask for your TAN (Federal Criminal Police Office).

One feature is enough to be suspicious. The BSI lists urgent calls to action, threats, requests for confidential data, links or forms, and unusual requests from known senders: if at least one applies, it is very likely phishing.

- The message arrives unexpectedly, for example from someone you rarely deal with (Microsoft).
- The "To" field contains many seemingly random recipients (Microsoft).
- The greeting is impersonal, such as "Dear customer" (Federal Criminal Police Office).

03 —

Check in Six Steps

How to clarify a suspicious message without using any link, attachment, or phone number from the message.

1

Pause

Don't reply, click, or pay right away. Urgency and threats are typical features of phishing (BSI).

2

Look at the sender

Move the mouse pointer over the sender line without clicking: is there a different address behind the name (BSI)? Odd spellings, numbers, or additions (Federal Criminal Police Office)?

3

Check the link target, don't click

Hover over the link, or press and hold it on a smartphone. An address is suspicious if it does not belong to the supposed organization, only imitates its name, or is a short link (Watchlist Internet, BSI).

4

Go there yourself instead of clicking

Open the sender's website or app via a bookmark or the known address instead of following the link (Federal Criminal Police Office).

5

Ask back through a known channel

Call, but using a number you looked up yourself, not the one in the message (BSI). This also applies to managers (Watchlist Internet).

6

Report if in doubt

Don't respond; report it through the internal reporting channel instead. That way, IT can warn others too (Watchlist Internet).

04 —

Special Forms: CEO Fraud, QR Codes, Text Messages, Calls, MFA

How to recognize fraud that does not look like a classic phishing email, and how to respond.

CEO fraud

Supposedly a manager, by email, phone, or video call, pushes for a quick, strictly confidential transfer; AI can imitate voice and face deceptively well. Warning signs: a private email address, a messenger, an unknown number, an unusual form of address. Hang up and call back through a known channel, even if the person is supposedly unreachable (Watchlist Internet).

QR code phishing (quishing)

A QR code in an email, supposedly from a bank or authority, is meant to solve an urgent problem and leads to malicious code or a fake input form. Virus scanners classify QR codes as harmless images. Don't scan it; contact the sender another way (BSI).

Text messages and chats (smishing)	Usually supposedly from a parcel service or shopping platform with a request for payment. Are you even expecting a parcel? If in doubt, don't click (BSI). Chats in Teams, Slack, Signal, or WhatsApp are also used (CISA).
Phone calls (vishing)	Supposedly a bank, the police, or IT support describes an emergency (BSI); the displayed number can be spoofed (CISA, Microsoft). Microsoft does not call unsolicited to provide support; scammers often ask for a remote access app (Microsoft). Don't give out anything, don't install anything, hang up (BSI).
Fake sign-in page	Looks like the real sign-in, for example for Microsoft 365. "https://" proves nothing (BSI), and such pages also intercept the six-digit one-time code (CISA). If known data such as your name or IBAN is requested again after sign-in, the page is probably fake (BSI).
MFA request you did not trigger	A confirmation prompt in the authenticator app when you are not signing in indicates that someone knows your password. Criminals send requests in series until someone approves by mistake or out of annoyance (CISA), or they ask for approval over the phone (BSI). Deny it and report it to IT immediately.

05

After a Click: Act Immediately

What to do immediately, depending on the situation. At work, inform IT first (Microsoft); IT decides on the next steps.

Immediate steps by situation (BSI, Federal Criminal Police Office, Watchlist Internet, Microsoft, CISA)

WHAT HAPPENED	WHAT YOU DO IMMEDIATELY
Link opened, nothing entered	Close the page, don't enter anything, report the message, and tell IT that you opened the link (CISA).
Credentials entered	Change the password immediately, via the real site or as instructed by IT, then end all active sessions and check for changed settings. Also secure accounts linked to this mailbox (BSI).
Attachment opened or remote access allowed	Inform IT immediately, preferably by phone. A device that scammers had access to should be reset (Microsoft).
MFA approved or code shared	Inform IT immediately: whoever received the approval may already be signed in (CISA).
Bank or card details entered	Have online banking, the account, and cards blocked, and monitor account activity (Federal Criminal Police Office).
Money transferred	Call your own bank immediately and try to stop the payment; file a report with the police (Watchlist Internet, Federal Criminal Police Office).

Reporting is not an admission of guilt: the sooner IT knows, the sooner accounts can be blocked and others warned. The table is a TOMORIS recommendation; your company's rules take precedence.

06 —

Report Correctly: Internally and in Austria

First the internal channel, then Outlook, Watchlist Internet, the cybercrime reporting office, and the police.

- Internal first: through your company's reporting channel, usually IT or the help desk. Microsoft recommends reporting threats to the security team immediately.
- Outlook: select the message, choose the built-in report button ("Report"), then "Report phishing." The message is deleted and, depending on the settings, sent to a reporting mailbox, to Microsoft, or to both; the button only appears in supported Outlook versions if your organization has set up the reporting feature (Microsoft Learn).
- Watchlist Internet: report phishing and other online traps using the reporting form on watchlist-internet.at; this helps protect others.
- Cybercrime reporting office of the Federal Criminal Police Office: against-cybercrime@bmi.gv.at if you suspect fraud. The report does not replace a criminal complaint; if damage has occurred, file a report with the police (Federal Criminal Police Office).
- Companies after a cyberattack: Cyber Security Hotline of the Austrian Economic Chamber (Wirtschaftskammer Österreich), 0800 888 133 (Federal Criminal Police Office).

Template: our reporting channels (fill in before sharing or posting)

REASON	CONTACT PERSON	PHONE OR EMAIL
Suspicious message, own click	_____	_____
IT emergency outside office hours	_____	_____
Confirm payment instructions or bank details	_____	_____
Your bank: stop payment, block account	_____	_____

07 —

Checklist to Post

Ten questions before every click, every entry, and every payment, as a TOMORIS recommendation.

- ☐ Am I expecting this message, and does the request fit the sender?
- ☐ Is the actual sender address correct, not just the displayed name?
- ☐ Am I being put under time pressure or threatened? Then check all the more.
- ☐ Does the link really lead to the organization that is writing? Hover over it, don't click.
- ☐ Am I supposed to open an attachment, enable macros, or install something? Ask first.

- ☐ Is a password, PIN, TAN, or one-time code being requested? Don't enter anything.
- ☐ Am I supposed to scan a QR code from an email? Don't scan it.
- ☐ An MFA request although I'm not signing in? Deny it and report it.
- ☐ Am I supposed to transfer money or change bank details? Ask first through a known channel.
- ☐ Supposed IT support wants remote access? Hang up and call your own IT.

08 —

For Managers and IT: Set the Framework

What managers and IT define so that employees report and your own domain is hard to spoof.

TOMORIS recommendations; check legal obligations, for example under the NISG 2026 (Austrian Network and Information Systems Security Act 2026), separately.

- Define the reporting channel and make it known; in Microsoft 365, enable the Outlook report button and define a reporting mailbox (Microsoft Learn).
- Train regularly: recognize suspicious emails and links, don't respond to them, and report opening them too (CISA). Welcome reports, including false alarms.
- Secure payments: whoever approves payments checks senders carefully and confirms unusual payment instructions through another communication channel (Watchlist Internet).
- Harden sign-in: phishing-resistant MFA based on FIDO or PKI; where that is not possible, push notifications with number matching (CISA).
- Protect your own domain: set DMARC for outgoing email to **reject** so that spoofed senders from your domain are rejected (CISA). The free email security check shows whether SPF, DKIM, and DMARC are set.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Email security check (German)
tomoris.com/tools/email-security-check

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact
contact@tomoris.com

09 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **BSI: How do I recognize phishing emails and websites?**
Recognizing phishing emails, recognizing phishing websites; accessed October 25, 2026
[www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cybe...](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber...)
- 2 **BSI: Phishing and its subtypes smishing, quishing, and vishing**
Smishing, quishing, vishing; accessed October 25, 2026
www.bsi.bund.de/dok/passwortdiebstahl-durch-phishing
- 3 **BSI and ProPK: Phishing, emergency checklist (PDF)**
What you should do if ...; How to protect yourself in the future
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Brosch...
- 4 **Federal Criminal Police Office: Phishing/Smishing fact sheet (PDF, October 2025)**
Warning signs, prevention recommendations, measures in case of damage
www.bundeskriminalamt.at/212/service/files/294_2025_infoblatt_p...
- 5 **Watchlist Internet: How to unmask telltale links**
Displaying links with a mouse and smartphone, suspicious addresses, reporting form
www.watchlist-internet.at/news/10tgp-links
- 6 **Watchlist Internet: When a deepfake calls instead of the executive floor**
CEO fraud, identifying features, my company is affected
www.watchlist-internet.at/news/auftrag-von-ganz-oben-wenn-sich-...
- 7 **Microsoft Learn: Report phishing and suspicious emails in Outlook**
Built-in button in Outlook; accessed October 25, 2026
learn.microsoft.com/de-de/defender-office-365/submissions-outlo...
- 8 **Microsoft Learn: How to protect yourself against phishing attacks**
Signs of a phishing scam, what to do
learn.microsoft.com/de-de/defender-endpoint/malware/phishing
- 9 **Microsoft Support: Tech support scams**
How scammers operate, how to protect yourself
support.microsoft.com/de-de/office/protect-yourself-from-tech-s...
- 10 **CISA, NSA, FBI, MS-ISAC: Phishing Guidance – Stopping the Attack Cycle at Phase One**
PDF pp. 4 to 6 (techniques, MFA, DMARC, training), p. 12 (reporting)
www.cisa.gov/resources-tools/resources/phishing-guidance-stoppi...