

SPICKZETTEL · TOMORIS TOOLBOX

Phishing erkennen: Spickzettel für Mitarbeitende

Warnzeichen, Prüfschritte und Sonderformen von Phishing, was nach einem Klick zu tun ist und wie Sie in Österreich richtig melden

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/phishing-erkennen-spickzettel

AUF EINEN BLICK

6

Warnzeichen mit Beispiel und Prüfweg

6

Sonderformen von CEO-Betrug bis MFA-Anfrage

10

Fragen zum Aushängen

10

Quellen: BSI, Bundeskriminalamt, Watchlist, Microsoft, CISA

FÜR WEN

- Alle Mitarbeitenden, die E-Mails, SMS, Chats und Anrufe bearbeiten, ohne IT-Vorwissen
- Führungskräfte, die den Spickzettel weitergeben, aushängen oder in Unterweisungen nutzen
- Buchhaltung, Einkauf und Assistenz, die Zahlungen auslösen oder freigeben
- IT-Verantwortliche, die Meldewege festlegen und Schulungen planen

WURUM ES GEHT

Phishing-Nachrichten wirken heute oft echt: gutes Deutsch, bekanntes Logo, scheinbar vertrauter Absender. Dieser Spickzettel zeigt die typischen Warnzeichen mit Beispiel und Prüfweg, die Sonderformen vom CEO-Betrug über QR-Codes und Anrufe bis zur MFA-Anfrage, die Sie nicht ausgelöst haben, und was nach einem Klick sofort zu tun ist. Dazu kommen die Meldewege in Österreich und eine Vorlage für Ihre internen Ansprechpersonen. Die Hinweise stützen sich auf BSI, Bundeskriminalamt, Watchlist Internet, Microsoft und CISA.

Dieser Spickzettel gibt einen Überblick und ersetzt keine Vorgaben Ihres Unternehmens. Tragen Sie Ihre internen Meldewege in die Vorlage ein, bevor Sie ihn weitergeben. Bezeichnungen und Funktionen in Outlook können je nach Version und Einstellung Ihrer IT abweichen; Kontaktdaten der Meldestellen mit Stand 25.10.2026.

INHALT

01	Die Grundregel: innehalten, prüfen, melden	2
02	Sechs Warnzeichen und wie Sie sie prüfen	3
03	In sechs Schritten prüfen	4
04	Sonderformen: CEO-Betrug, QR-Codes, SMS, Anrufe, MFA	4
05	Nach einem Klick: sofort handeln	5
06	Richtig melden: intern und in Österreich	6
07	Checkliste zum Aushängen	7
08	Für Führungskräfte und IT: den Rahmen setzen	7
09	Quellen	8

01

Die Grundregel: innehalten, prüfen, melden

Phishing kommt per E-Mail, SMS, Chat, Anruf oder QR-Code. Gutes Deutsch ist keine Entwarnung.

Innehalten

Druck ist das Warnsignal

Dringender Handlungsbedarf und angedrohte Konsequenzen sind typische Merkmale (BSI, Bundeskriminalamt).

Prüfen

Über einen anderen Weg

Nicht über Link oder Nummer aus der Nachricht, sondern über selbst herausgesuchte Kontaktdaten (BSI).

Melden

Auch den eigenen Klick

Auch geöffnete verdächtige E-Mails, Links und Anhänge melden, so früh wie möglich (CISA).

Phishing-Nachrichten geben sich als bekannte Person oder Organisation aus, etwa als Bank, Paketdienst, Behörde, Vorgesetzte oder IT-Abteilung, und sollen Sie dazu bringen, einen Link zu öffnen, einen Anhang zu starten, Zugangsdaten einzugeben oder Geld zu überweisen (BSI, CISA). Fehlerfreier Text ist kein Echtheitsbeweis: Tippfehler sind laut BSI nur noch selten ein eindeutiger Hinweis. Achten Sie auf das Anliegen, nicht auf die Sprache.

02

Sechs Warnzeichen und wie Sie sie prüfen

Absender, Druck, Links, Anhänge, ungewöhnliche Bitten und abgefragte Daten: Merkmal, Beispiel und Prüfweg.

Warnzeichen in E-Mails, SMS und Chats (BSI, Bundeskriminalamt, Watchlist Internet, Microsoft)

MERKMAL	BEISPIEL	SO PRÜFEN SIE
Absender passt nicht	Anzeigenname „IT-Service“, dahinter eine fremde Adresse; Domain mit zusätzlichen Zahlen oder geänderten Buchstaben	Mauszeiger auf die Absenderzeile legen, ohne zu klicken: Dahinter kann eine andere Adresse stehen (BSI). Passt die Signatur nicht zur Adresse, ist das ein Warnzeichen (Microsoft).
Druck und Drohung	„Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren ...“	Nicht unter Druck setzen lassen (Bundeskriminalamt). Das Anliegen selbst über die bekannte Website oder Nummer klären.
Link führt woanders hin	Button „Konto bestätigen“, dahinter eine wilde Zeichenfolge, ein Kurzlink oder eine Adresse wie „www.135x-Bank.de“	Mauszeiger auf den Link legen, am Smartphone den Finger darauf lassen: Die echte Zieladresse erscheint (Watchlist Internet). „https://“ ist keine Entwarnung (BSI).
Unerwarteter Anhang	Endung .exe oder .scr, doppelte Endung wie .pdf.exe, Aufforderung, Makros zu aktivieren	Anhänge verdächtiger E-Mails nicht öffnen (BSI). Verlangt eine Datei, Makros zu aktivieren oder etwas zu installieren, ist das ein deutliches Anzeichen (Microsoft).
Ungewöhnliche Bitte	Die Geschäftsführung schreibt von einer privaten Adresse und verlangt eine eilige, vertrauliche Überweisung	Misstrauisch werden, wenn ein bekannter Absender ein ungewöhnliches Anliegen hat (BSI). Die Person über einen bekannten Weg zurückrufen (Watchlist Internet).
Vertrauliche Daten verlangt	Passwort, PIN, TAN oder Kreditkartennummer per E-Mail, SMS, Formular oder Telefon	Banken und Behörden fragen nie per E-Mail nach Ihrem Passwort (BSI), Bankmitarbeitende nie nach der TAN (Bundeskriminalamt).

Ein Merkmal genügt für Misstrauen. Das BSI nennt dringenden Handlungsbedarf, Drohungen, die Abfrage vertraulicher Daten, Links oder Formulare und ungewöhnliche Anliegen bekannter Absender: Trifft mindestens eines zu, handelt es sich mit hoher Wahrscheinlichkeit um Phishing.

- Die Nachricht kommt unerwartet, etwa von jemandem, mit dem Sie selten zu tun haben (Microsoft).
- Im Feld „An“ stehen viele scheinbar zufällige Empfänger (Microsoft).
- Die Anrede ist unpersönlich, etwa „Sehr geehrte Kundin / Sehr geehrter Kunde“ (Bundeskriminalamt).

03 —

In sechs Schritten prüfen

So klären Sie eine verdächtige Nachricht, ohne Link, Anhang oder Telefonnummer aus der Nachricht zu benutzen.

1

Innehalten

Nicht sofort antworten, klicken oder zahlen. Dringlichkeit und Drohungen sind typische Merkmale von Phishing (BSI).

2

Absender ansehen

Mauszeiger über die Absenderzeile führen, ohne zu klicken: Steckt hinter dem Namen eine andere Adresse (BSI)? Seltsame Schreibweisen, Zahlen oder Ergänzungen (Bundeskriminalamt)?

3

Linkziel prüfen, nicht klicken

Mauszeiger auf den Link legen, am Smartphone den Finger darauf lassen. Verdächtig ist eine Adresse, die nicht zur angeblichen Organisation gehört, den Namen nur nachahmt oder ein Kurzlink ist (Watchlist Internet, BSI).

4

Selbst aufrufen statt klicken

Website oder App des Absenders über ein Lesezeichen oder die bekannte Adresse öffnen, statt dem Link zu folgen (Bundeskriminalamt).

5

Über einen bekannten Kanal rückfragen

Anrufen, aber unter einer selbst herausgesuchten Nummer, nicht unter der aus der Nachricht (BSI). Das gilt auch für Vorgesetzte (Watchlist Internet).

6

Bei Zweifel melden

Nicht reagieren, sondern über den internen Meldeweg melden. So kann die IT auch andere warnen (Watchlist Internet).

04 —

Sonderformen: CEO-Betrug, QR-Codes, SMS, Anrufe, MFA

Woran Sie Betrug erkennen, der nicht wie eine klassische Phishing-Mail aussieht, und wie Sie reagieren.

CEO-Betrug

Angeblich die Führungskraft drängt per Mail, Anruf oder Videocall auf eine rasche, streng vertrauliche Überweisung; Stimme und Gesicht lassen sich mit KI täuschend echt nachahmen. Warnzeichen: private E-Mail-Adresse, Messenger, unbekannte Nummer, ungewohnte Anrede. Auflegen und über einen bekannten Weg zurückrufen, auch wenn die Person angeblich nicht erreichbar ist (Watchlist Internet).

QR-Code-Phishing (Quishing)	Ein QR-Code in einer E-Mail, angeblich von Bank oder Behörde, soll ein dringendes Problem lösen und führt auf Schadcode oder eine gefälschte Eingabemaske. Virens Scanner stufen QR-Codes als harmloses Bild ein. Nicht scannen, den Absender auf anderem Weg kontaktieren (BSI).
SMS und Chats (Smishing)	Meist angeblich vom Paketdienst oder von Shopping-Plattformen mit Zahlungsaufforderung. Erwarten Sie überhaupt ein Paket? Im Zweifel nicht klicken (BSI). Auch Chats in Teams, Slack, Signal oder WhatsApp werden genutzt (CISA).
Anrufe (Vishing)	Angeblich Bank, Polizei oder IT-Support schildert eine Notsituation (BSI); die angezeigte Nummer kann gefälscht sein (CISA, Microsoft). Microsoft ruft nicht unaufgefordert an, um Support zu leisten; Betrüger verlangen oft eine App für den Fernzugriff (Microsoft). Nichts herausgeben, nichts installieren, auflegen (BSI).
Gefälschte Anmeldeseite	Sieht aus wie die echte Anmeldung, etwa für Microsoft 365. „https://“ beweist nichts (BSI), und solche Seiten fangen auch den sechsstelligen Einmalcode ab (CISA). Werden nach der Anmeldung bekannte Daten wie Name oder IBAN erneut verlangt, ist die Seite wahrscheinlich gefälscht (BSI).
MFA-Anfrage, die Sie nicht ausgelöst haben	Eine Bestätigung in der Authenticator-App, obwohl Sie sich nicht anmelden, deutet darauf hin, dass jemand Ihr Passwort kennt. Kriminelle senden Anfragen in Serie, bis jemand versehentlich oder genervt bestätigt (CISA), oder bitten am Telefon darum (BSI). Ablehnen und sofort der IT melden.

05

Nach einem Klick: sofort handeln

Was Sie je nach Lage sofort tun. Am Arbeitsplatz zuerst die IT informieren (Microsoft), sie entscheidet über die nächsten Schritte.

Sofortmaßnahmen nach Lage (BSI, Bundeskriminalamt, Watchlist Internet, Microsoft, CISA)

WAS PASSIERT IST	WAS SIE SOFORT TUN
Link geöffnet, nichts eingegeben	Seite schließen, nichts eingeben, Nachricht melden und der IT sagen, dass Sie den Link geöffnet haben (CISA).
Zugangsdaten eingegeben	Passwort sofort ändern, über die echte Seite oder nach Anleitung der IT, danach alle aktiven Sitzungen beenden und geänderte Einstellungen prüfen. Konten, die mit diesem Postfach verknüpft sind, ebenfalls absichern (BSI).
Anhang geöffnet oder Fernzugriff erlaubt	Sofort die IT informieren, am besten telefonisch. Ein Gerät, auf das Betrüger Zugriff hatten, sollte zurückgesetzt werden (Microsoft).
MFA bestätigt oder Code weitergegeben	Sofort die IT informieren: Wer die Bestätigung erhalten hat, kann bereits angemeldet sein (CISA).
Bank- oder Kartendaten eingegeben	Online-Banking, Konto und Karten sperren lassen und Kontobewegungen überwachen (Bundeskriminalamt).

Geld überwiesen

Sofort die eigene Bank anrufen und versuchen, die Zahlung zu stoppen; Anzeige bei der Polizei erstatten (Watchlist Internet, Bundeskriminalamt).

Melden ist kein Schuldeingeständnis: Je früher die IT Bescheid weiß, desto eher lassen sich Konten sperren und andere warnen. Die Tabelle ist eine Empfehlung von TOMORIS; die Vorgaben Ihres Unternehmens gehen vor.

06

Richtig melden: intern und in Österreich

Zuerst der interne Weg, dann Outlook, Watchlist Internet, die Cybercrime-Meldestelle und die Polizei.

- Intern zuerst: über den Meldeweg Ihres Unternehmens, meist IT oder Helpdesk. Microsoft empfiehlt, Bedrohungen sofort dem Sicherheitsteam zu melden.
- Outlook: Nachricht markieren, die integrierte Schaltfläche zum Melden wählen (englisch „Report“), dann „Phishing melden“. Die Nachricht wird gelöscht und je nach Einstellung an ein Meldepostfach, an Microsoft oder an beide übermittelt; die Schaltfläche erscheint nur in unterstützten Outlook-Versionen, wenn Ihre Organisation die Meldefunktion eingerichtet hat (Microsoft Learn).
- Watchlist Internet: Phishing und andere Internetfallen über das Meldeformular auf watchlist-internet.at melden; das hilft, andere zu schützen.
- Cybercrime-Meldestelle des Bundeskriminalamts: against-cybercrime@bmi.gv.at bei Betrugsverdacht. Die Meldung ersetzt keine Anzeige; ist ein Schaden entstanden, Anzeige bei der Polizei erstatten (Bundeskriminalamt).
- Unternehmen nach einem Cyberangriff: Cyber-Security-Hotline der Wirtschaftskammer Österreich, 0800 888 133 (Bundeskriminalamt).

Vorlage: unsere Meldewege (vor dem Weitergeben oder Aushängen ausfüllen)

ANLASS	ANSPRECHPERSON	TELEFON ODER E-MAIL
Verdächtige Nachricht, eigener Klick	_____	_____
IT-Notfall außerhalb der Bürozeiten	_____	_____
Zahlungsanweisung oder Bankdaten bestätigen	_____	_____
Hausbank: Zahlung stoppen, Konto sperren	_____	_____

07 —

Checkliste zum Aushängen

Zehn Fragen vor jedem Klick, jeder Eingabe und jeder Zahlung, als Empfehlung von TOMORIS.

- ☐ Erwarte ich diese Nachricht, und passt das Anliegen zum Absender?
- ☐ Stimmt die tatsächliche Absenderadresse, nicht nur der angezeigte Name?
- ☐ Werde ich unter Zeitdruck gesetzt oder bedroht? Dann erst recht prüfen.
- ☐ Führt der Link wirklich zur Organisation, die schreibt? Mauszeiger darauf, nicht klicken.
- ☐ Soll ich einen Anhang öffnen, Makros aktivieren oder etwas installieren? Erst rückfragen.
- ☐ Werden Passwort, PIN, TAN oder Einmalcode verlangt? Nichts eingeben.
- ☐ Soll ich einen QR-Code aus einer E-Mail scannen? Nicht scannen.
- ☐ MFA-Anfrage, ohne dass ich mich anmelde? Ablehnen und melden.
- ☐ Soll ich Geld überweisen oder Bankdaten ändern? Erst über einen bekannten Weg rückfragen.
- ☐ Angeblicher IT-Support will Fernzugriff? Auflegen und die eigene IT anrufen.

08 —

Für Führungskräfte und IT: den Rahmen setzen

Was Führungskräfte und IT festlegen, damit Mitarbeitende melden und die eigene Domain schwer zu fälschen ist.

Empfehlungen von TOMORIS; gesetzliche Pflichten, etwa nach dem NISG 2026, prüfen Sie gesondert.

- Meldeweg festlegen und bekannt machen; in Microsoft 365 die Outlook-Schaltfläche zum Melden aktivieren und ein Meldepostfach festlegen (Microsoft Learn).
- Regelmäßig schulen: verdächtige E-Mails und Links erkennen, nicht darauf reagieren und auch das Öffnen melden (CISA). Meldungen positiv aufnehmen, auch Fehlalarme.
- Zahlungen absichern: Wer Zahlungen freigibt, prüft Absender genau und bestätigt auffällige Zahlungsanweisungen über einen anderen Kommunikationsweg (Watchlist Internet).
- Anmeldung härten: phishing-resistente MFA auf Basis von FIDO oder PKI; wo das nicht geht, Push-Bestätigungen mit Nummernabgleich (CISA).
- Eigene Domain schützen: DMARC für ausgehende E-Mails auf **reject** setzen, damit gefälschte Absender Ihrer Domain abgewiesen werden (CISA). Ob SPF, DKIM und DMARC gesetzt sind, zeigt der kostenlose E-Mail-Sicherheits-Check.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

E-Mail-Sicherheits-Check

tomoris.com/tools/email-security-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- BSI: Wie erkenne ich Phishing-E-Mails und -Webseiten?**
Phishing-E-Mails erkennen, Phishing-Webseiten erkennen; gelesen am 25.10.2026
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cybe...
- BSI: Phishing und seine Unterarten Smishing, Quishing und Vishing**
Smishing, Quishing, Vishing; gelesen am 25.10.2026
www.bsi.bund.de/dok/passwortdiebstahl-durch-phishing
- BSI und ProPK: Phishing, Checkliste für den Ernstfall (PDF)**
Das sollten Sie tun, wenn ...; So schützen Sie sich in Zukunft
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Brosc...
- Bundeskriminalamt: Infoblatt Phishing/Smishing (PDF, Oktober 2025)**
Warnsignale, Präventionsempfehlungen, Maßnahmen im Schadensfall
www.bundeskriminalamt.at/212/service/files/294_2025_infoblatt_p...
- Watchlist Internet: So enttarnen Sie verräterische Links**
Link anzeigen mit Maus und Smartphone, verdächtige Adressen, Meldeformular
www.watchlist-internet.at/news/10tgp-links
- Watchlist Internet: Wenn sich statt der Chefetage ein Deepfake meldet**
CEO-Betrug, Erkennungsmerkmale, Mein Unternehmen ist betroffen
www.watchlist-internet.at/news/auftrag-von-ganz-oben-wenn-sich-...
- Microsoft Learn: Melden von Phishing und verdächtigen E-Mails in Outlook**
Integrierte Schaltfläche in Outlook; gelesen am 25.10.2026
learn.microsoft.com/de-de/defender-office-365/submissions-outlo...
- Microsoft Learn: So schützen Sie sich vor Phishing-Angriffen**
Anzeichen eines Phishing-Betrugs, Was zu tun ist
learn.microsoft.com/de-de/defender-endpoint/malware/phishing
- Microsoft Support: Betrugsversuche im Zusammenhang mit dem technischen Support**
Vorgehensweise der Betrüger, So schützen Sie sich
support.microsoft.com/de-de/office/protect-yourself-from-tech-s...
- CISA, NSA, FBI, MS-ISAC: Phishing Guidance – Stopping the Attack Cycle at Phase One**
PDF S. 4 bis 6 (Techniken, MFA, DMARC, Schulung), S. 12 (Reporting)
www.cisa.gov/resources-tools/resources/phishing-guidance-stoppi...