

Phishing Notfallkarte

Für Mitarbeitende: verdächtige Nachrichten prüfen, sicher melden und nach einem möglichen Fehler schnell reagieren. IT oder Informationssicherheit ergänzt vor der Verteilung die internen Meldewege.

Vor dem Klick

Unerwartete Aufforderung, Zeitdruck, neue Bankverbindung oder Bitte um Zugangsdaten? Kurz stoppen. Auch eine bekannte Absenderadresse und fehlerfreie Sprache beweisen keine Echtheit.

Anliegen über einen bekannten Kontakt oder eine selbst geöffnete offizielle App prüfen. Keine Rufnummer, Antwortfunktion oder Anmeldung aus der verdächtigen Nachricht verwenden.

Links, Anhänge und QR-Ziele nicht zum Ausprobieren öffnen. Keine Passwörter oder MFA-Codes weitergeben; unerwartete MFA-Anfragen ablehnen.

Verdacht intern melden

Vorgesehenen Meldebutton oder vereinbarten IT-Kontakt nutzen. Zeitpunkt, betroffenen Dienst und eigene Aktionen nennen. Nachricht nach interner Vorgabe sichern oder melden; nicht an Kolleginnen und Kollegen weiterverbreiten. Nicht auf den Absender reagieren.

Schon etwas getan

Situation	Jetzt handeln
Link geöffnet	Interaktion beenden, nichts weiter eingeben und IT zeitnah informieren. Ein Klick allein beweist keine Infektion; IT bewertet die Lage.
Passwort oder MFA bestätigt	Sofort IT melden. Betroffene Passwörter über einen bekannten Zugang von einem vertrauenswürdigen Gerät ändern, auch bei Wiederverwendung. IT soll aktive Sitzungen und Kontozugriffe prüfen und gegebenenfalls sperren.
Datei geöffnet oder Geld gesendet	Sofort IT kontaktieren und Anweisungen zum betroffenen Gerät befolgen. Keine eigenständige Bereinigung oder Löschung von Belegen. Bei Zahlung zusätzlich Finanzverantwortliche und Bank über bekannte Kontaktdaten erreichen.

Meldestelle / Meldebutton: _____

Ersatzkontakt und Telefon: _____

Interne Phishing Meldung

Diese Vorlage unterstützt die Übergabe an IT. Melden Sie dringende Fälle sofort über den vereinbarten Weg; warten Sie nicht, bis alle Felder ausgefüllt sind.

Angabe	Eintrag
Zeitpunkt und eigener Rückkontakt	
Kanal und Absenderangabe	
Betreff oder kurze Beschreibung	
Betroffenes Konto oder Gerät	
Eigene Aktionen und Zeitpunkt	
Beobachtete Folgen oder Warnungen	
Bereits informierte Stelle und Vorgangsnummer	

Keine Passwörter, MFA-Codes oder vollständigen Kundendaten eintragen. Originalnachrichten und Anhänge nur über den von IT freigegebenen Meldeweg übergeben.

Beispiel einer kurzen Meldung

Fiktives Beispiel: „09:15 Uhr, E-Mail angeblich vom Lieferanten zur Änderung der Bankverbindung. Ich habe die Nachricht gelesen, keinen Link geöffnet und keine Zahlung ausgelöst. Bitte um Prüfung. Rückkontakt über den internen Dienstkontakt.“

Anpassen und weitergeben

Eigene Vorlage der Paragamix GmbH. Kostenlos intern nutzen, anpassen und an Kunden weitergeben. Interne Kontakte und Abläufe vor Nutzung ergänzen und prüfen. Ein Quellenlink ist willkommen, aber keine Voraussetzung.

[NIST Phishing](#) | [BSI CSN Leitfaden](#)

[Aktuelle Fassung und Werkzeuge](#)