

Phishing-Mails erkennen

Ein Leitfaden von IT Logic: it-logic.de

Merkblatt: Phishing erkennen in 60 Sekunden

Bevor Sie klicken, fragen Sie sich:

1. Habe ich diese Nachricht erwartet?
2. Passt der Absender wirklich, und stimmt die komplette Adresse?
3. Wird Druck aufgebaut oder mit Folgen gedroht?
4. Soll ich etwas anklicken, öffnen, eingeben oder überweisen?
5. Wohin führt der Link, wenn ich mit der Maus darüberfahre?

Goldene Regeln:

- Keine Passwörter oder Codes per Mail oder Telefon herausgeben.
- Anmeldungen nur über Lesezeichen oder selbst eingegebene Adressen.
- Anhänge nur öffnen, wenn sie erwartet wurden.
- Bankdaten-Änderungen immer telefonisch bestätigen.
- Bei Zweifel: nicht klicken, melden, nachfragen.

Meldeweg: Melde-Button im Mailprogramm oder Weiterleitung an *[Adresse der IT einfügen]*, bei Eilfällen Telefon *[Nummer einfügen]*.

Checkliste: Verdächtige Nachricht

Gehen Sie die Punkte der Reihe nach durch. Sobald Sie mehrere Fragen mit „Ja“ beantworten, behandeln Sie die Nachricht als verdächtig.

Absender

- Weicht die Absenderadresse vom erwarteten Muster ab?
- Passt der Anzeigename nicht zur tatsächlichen Adresse?
- Kommt die Nachricht von einem privaten Postfach, obwohl sie dienstlich sein soll?

Inhalt

- Ist die Nachricht unerwartet?
- Wird Druck ausgeübt, mit Sperrung oder Strafe gedroht?
- Wird nach Passwörtern, Codes oder Zahlungsdaten gefragt?
- Wird um Vertraulichkeit oder Umgehung üblicher Wege gebeten?

Links und Anhänge

- Unterscheiden sich Linktext und tatsächliches Ziel?
- Enthält der Link eine ungewöhnliche oder leicht veränderte Domain?
- Gibt es einen unerwarteten Anhang oder die Aufforderung, Makros zu aktivieren?

- Befindet sich ein QR-Code in der Nachricht?

Nächste Schritte

- Nicht klicken, nicht antworten.
- Nachricht melden.
- Bei Zahlungen: telefonisch über bekannte Nummer zurückfragen.

Wissens-Quiz mit Lösungen

Frage 1: Eine Mail Ihrer Geschäftsführung bittet vom privaten Postfach aus um eine dringende, vertrauliche Überweisung. Was tun Sie? a) Sofort überweisen, es ist ja der Chef b) Antworten und um Bestätigung bitten c) Die Person über eine bekannte Nummer kontaktieren und die IT informieren d) Die Mail ignorieren und nichts weiter tun

Frage 2: Woran erkennen Sie die echte Domain in einer Internetadresse am besten? a) Am Schloss-Symbol im Browser b) An dem Teil direkt vor dem ersten einzelnen Schrägstrich, von hinten gelesen c) An der Länge der Adresse d) Am Firmennamen am Anfang der Adresse

Frage 3: Sind Rechtschreibfehler ein sicheres Zeichen für Phishing? a) Ja, immer b) Nein, sie sind ein Hinweis, aber auch fehlerfreie Mails können betrügerisch sein c) Nur bei E-Mails aus dem Ausland d) Nur bei Mails mit Anhang

Frage 4: Sie erhalten auf dem Smartphone mehrfach eine Anmeldebestätigung, obwohl Sie sich nicht anmelden wollten. Was tun Sie? a) Bestätigen, damit die Meldungen aufhören b) Ignorieren, bis es aufhört c) Ablehnen und die IT sofort informieren d) Das Gerät ausschalten und nichts weiter tun

Frage 5: Ein bekannter Lieferant teilt per Mail eine neue Bankverbindung mit. Wie gehen Sie vor? a) Die neue Bankverbindung direkt übernehmen b) Auf die Mail antworten und um Bestätigung bitten c) Telefonisch unter einer bereits bekannten Nummer rückfragen, bevor gezahlt wird d) Die Rechnung auf beide Konten aufteilen

Frage 6: Ein Word-Dokument fordert Sie auf, „Inhalte zu aktivieren“, um den Text zu sehen. Was tun Sie? a) Aktivieren, sonst kann ich nicht arbeiten b) Nicht aktivieren, das Dokument melden und die Herkunft prüfen c) Das Dokument an Kollegen weiterleiten d) Auf dem privaten Gerät öffnen

Frage 7: Was bedeutet das Schloss-Symbol im Browser? a) Die Seite ist garantiert seriös b) Die Verbindung ist verschlüsselt, mehr nicht c) Die Seite wurde vom Staat geprüft d) Die Seite enthält keine Schadsoftware

Frage 8: Sie haben auf einen verdächtigen Link geklickt und Ihr Passwort eingegeben. Was ist jetzt am wichtigsten? a) Abwarten, ob etwas passiert b) Sofort die IT informieren und Passwörter ändern c) Die Mail löschen und niemandem etwas sagen d) Den Browser neu starten

Frage 9: Ein Anrufer gibt sich als IT-Support aus und bittet Sie, ein Programm für Fernwartung zu installieren. Was tun Sie? a) Installieren, es ist ja der Support b) Auflegen, selbst bei der IT unter bekannter Nummer zurückrufen c) Dem Anrufer ein Einmalpasswort durchgeben d) Den Kollegen am Nachbartisch bitten, es zu erledigen

Frage 10: Warum ist es wichtig, auch Fehlklicks zu melden? a) Damit die Schuldigen bestraft werden können b) Weil schnelles Handeln den Schaden begrenzt c) Weil es vorgeschrieben ist, auch wenn es nichts bringt d) Es ist nicht wichtig

Lösungen:

Frage	Richtige Antwort	Kurze Begründung
1	c	Typisches Muster für Chef-Betrug, Rückfrage über unabhängigen Weg ist Pflicht.
2	b	Vor dem ersten einzelnen Schrägstrich, von hinten gelesen, steht die tatsächliche Domain.
3	b	Fehler sind ein Hinweis, aber kein verlässlicher Test.
4	c	Das ist ein Hinweis auf gestohlene Zugangsdaten oder MFA-Müdigkeits-Angriff.
5	c	Nur eine Rückfrage über bekannte Wege schützt vor Zahlungsbetrug.
6	b	Aktivierungsaufforderungen sind ein klassischer Weg für Schadsoftware.
7	b	Verschlüsselung sagt nichts über die Vertrauenswürdigkeit aus.
8	b	Schnelle Meldung und Passwortwechsel begrenzen den Schaden.
9	b	Echte Support-Mitarbeiter rufen nicht unaufgefordert an und verlangen keine Fernwartung.
10	b	Je früher die IT reagiert, desto geringer der Schaden.

Vorlage: Meldeprozess bei Phishing

Ziel: Jeder Mitarbeiter weiß, wie er einen Phishing-Verdacht schnell und ohne Angst melden kann.

Schritt 1: Erkennen. Nachricht, Anruf oder SMS erscheint verdächtig.

Schritt 2: Nicht interagieren. Nicht klicken, nicht antworten, nichts öffnen oder eingeben.

Schritt 3: Melden.

- Über den Melde-Button im Mailprogramm oder
- per Weiterleitung als Anhang an *[Adresse der IT einfügen]* oder
- bei Eilfällen telefonisch an *[Nummer einfügen]*, erreichbar *[Zeiten einfügen]*

Schritt 4: Rückmeldung. Die IT bestätigt den Eingang und teilt mit, ob die Nachricht gefährlich war.

Schritt 5: Maßnahmen. Die IT prüft, ob weitere Empfänger betroffen sind, sperrt gegebenenfalls Absender und Links und informiert bei Bedarf die Belegschaft.

Schritt 6: Dokumentation. Der Vorfall wird kurz festgehalten (Datum, Art, Maßnahmen). Bei Verdacht auf Datenabfluss wird umgehend der Datenschutzbeauftragte eingebunden, damit Meldefristen eingehalten werden.

Sonderfall: Bereits geklickt oder Daten eingegeben

- Sofort telefonisch die IT informieren
- Gerät vom Netzwerk trennen, aber nicht ausschalten, solange die IT nichts anderes sagt
- Passwörter von einem sicheren Gerät aus ändern lassen oder selbst ändern
- Keine Schuldzuweisung: Schnelle Meldung ist erwünscht und wird positiv bewertet

Sonderfall: Zahlung ausgelöst

- Sofort Buchhaltung und Geschäftsführung informieren
- Die Bank des Unternehmens unverzüglich kontaktieren
- Beweise sichern (Mail, Kontodaten, Zeitpunkt)

Gliederung für eine 45-Minuten-Schulung

Zeit	Inhalt	Methode
0 bis 5 Minuten	Begrüßung, Ziel, warum Phishing alle betrifft	Kurzer Einstieg mit anonymisiertem Beispiel aus dem eigenen Haus
5 bis 15 Minuten	Formen von Phishing und typische Warnsignale	Vortrag mit Bildbeispielen
15 bis 25 Minuten	STOPP-Methode, Links und Anhänge prüfen	Gemeinsame Übung an Beispielmails
25 bis 35 Minuten	Meldeweg und richtiges Verhalten nach einem Klick	Durchgang des Meldeprozesses, Fragen
35 bis 43 Minuten	Wissens-Quiz	Gruppenarbeit oder interaktive Abfrage
43 bis 45 Minuten	Zusammenfassung und Merkblatt verteilen	Kurzfazit

Tipp zur Durchführung: Beginnen Sie mit einer Frage an die Teilnehmer („Wer hat schon einmal eine verdächtige Mail erhalten?“). So wird deutlich, dass alle betroffen sind und niemand sich schämen muss.

13. Häufige Fragen

Kann ich durch das bloße Öffnen einer Phishing-Mail infiziert werden? In der Regel nicht. Gefährlich sind vor allem Klicks auf Links, geöffnete Anhänge und eingegebene Daten. Dennoch sollten verdächtige Mails nicht unnötig geöffnet, sondern direkt gemeldet werden.

Muss ich jede Mail misstrauisch prüfen? Nein. Es genügt, bei Nachrichten mit einer Handlungsaufforderung (klicken, öffnen, zahlen, Daten eingeben) kurz innezuhalten. Die STOPP-Methode dauert nur wenige Sekunden.

Was, wenn die Mail von einem Kollegen oder Kunden kommt, den ich kenne? Auch bekannte Absender können gehackt oder gefälscht sein. Bei ungewöhnlichen Bitten fragen Sie über einen zweiten Weg nach, etwa telefonisch oder im persönlichen Gespräch.

Wie erkenne ich Phishing am Smartphone? Dort sind Absenderadressen und Linkziele schlechter sichtbar. Halten Sie Links gedrückt, um das Ziel anzuzeigen, und öffnen Sie sensible Anmeldungen lieber über die offizielle App oder ein Lesezeichen.

Wie oft sollte geschult werden? Empfehlenswert ist eine Grundschulung bei Eintritt ins Unternehmen sowie regelmäßige kurze Auffrischungen, ergänzt um aktuelle Hinweise, wenn neue Betrugswellen auftreten.

Was ist, wenn ich mir nicht sicher bin, ob eine Mail echt ist? Dann melden Sie sie. Eine unnötige Meldung kostet wenig, eine übersehene Phishing-Mail kann sehr teuer werden.

Dürfen Unternehmen Phishing-Simulationen durchführen? Grundsätzlich ja, aber unter Beachtung von Datenschutz und Mitbestimmung. Informieren Sie die Belegschaft, binden Sie Datenschutzbeauftragten und gegebenenfalls Betriebsrat ein und nutzen Sie die Ergebnisse zum Lernen statt zur Sanktion.

Weitere Frage?

Kontaktieren Sie uns: it-logic.de/kontakt