

So erkennen Sie Phishing-Mails

PHISHING-MAILS. Jeder einzelne Bestandteil einer verdächtigen E-Mail kann Ihnen Anhaltspunkte geben. Am besten, indem Sie sich Kontrollfragen stellen.

! Zu «Von:»

- Kennen Sie den Absender?
- Haben Sie mit diesem Absender üblicherweise Kontakt via Mail?
- Ist das überhaupt seine E-Mail-Adresse? (Der angezeigte Name kann täuschen. Wenn Sie mit dem Cursor über die Adresse des Absenders fahren, wird in manchen Mailprogrammen die hinterlegte E-Mail-Adresse angezeigt.)
- Bei vermeintlich offiziellen Absendern: Ist die E-Mail-Adresse plausibel?

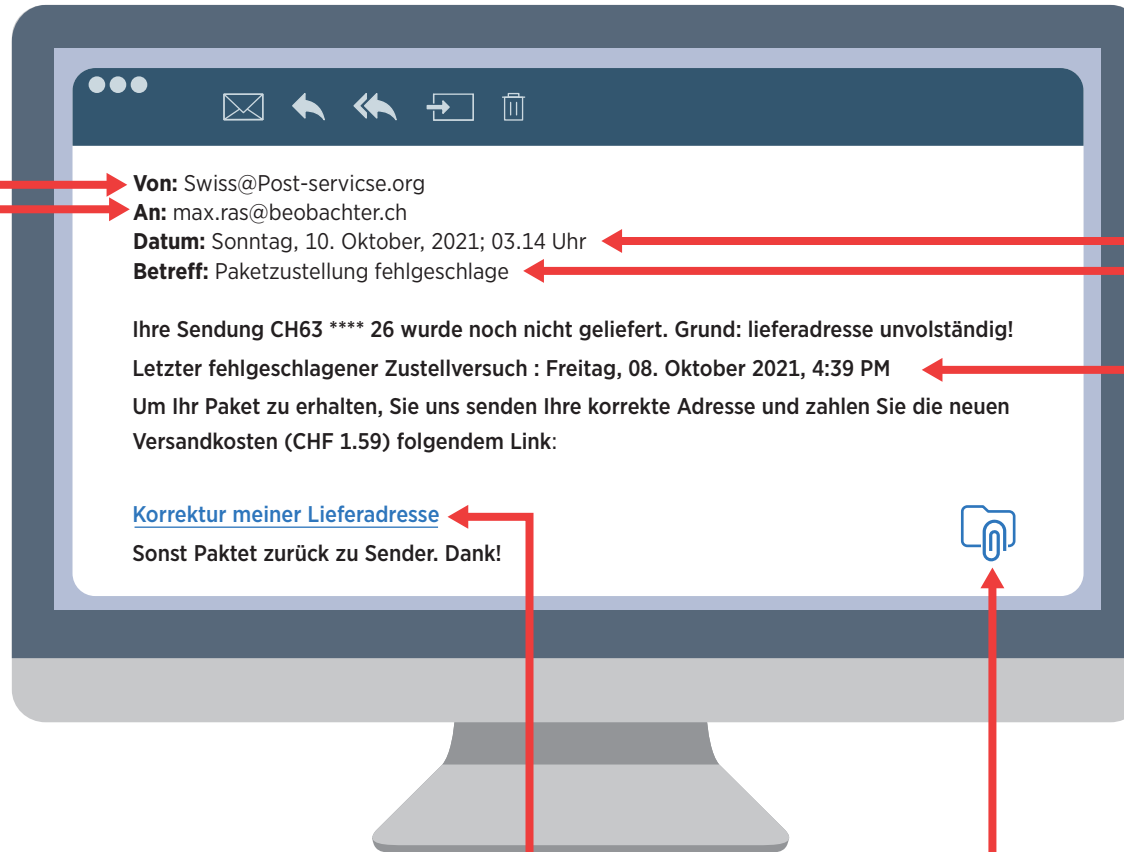
! Zu «An:» und «Cc:»

- Kennen Sie die anderen Empfänger/-innen? (Auch jene im Cc?)
- Ist die Zusammensetzung der Empfängerliste ungewöhnlich oder unplausibel?
- Gibt es andere Auffälligkeiten? (Zum Beispiel: Alle Empfänger/-innen beginnen mit dem gleichen Buchstaben)

Weitere Tipps

- Reagieren Sie nicht auf offensichtlichen Spam. Sonst wissen die Betrüger, dass Sie die Mail erhalten und angeschaut haben.
- Klicken Sie bei Spam auch nicht auf Unsubscribe-Links, damit bestätigen Sie nur Ihre E-Mail-Adresse.
- Für besonders starken Schutz deaktivieren Sie im Mailprogramm die automatische Vorschau.

Mehr Tipps zur digitalen Selbstverteidigung finden Sie hier:



! Zu Datum und Uhrzeit

- Ist der Zeitpunkt des Eintreffens bei diesem Absender plausibel? (In der Regel ist etwa sonntags oder nachts keine geschäftliche Korrespondenz zu erwarten.)

! Zu «Betreff:»

- Macht die Betreffzeile klar, worum es in der Mail geht, oder bleibt sie vage?
- Betrifft Sie der beschriebene Sachverhalt/das Thema wirklich?
- Gibt die Betreffzeile vor, eine Antwort auf eine E-Mail oder eine Anfrage zu sein («RE:» im Betreff), die Sie nie versandt haben?
- Ist dieses Thema für Sie relevant?
- Passen Betreffzeile und Inhalt zusammen?

! Zum Inhalt

- Weist der Text ungewohnt viele Schreibfehler oder schlechte Grammatik auf, die auf ein Übersetzungsprogramm hinweisen könnten?
- Enthält die E-Mail lediglich einen Link oder eine Datei?
- Ist die Nachricht wirklich an Sie gerichtet, oder klingt sie eher allgemein?
- Werden Sie mit Versprechungen (Geld, Gewinnbeteiligung, Geheimtipp) geködert?
- Wird Ihnen (unterschwellig) gedroht? (Unglück abwenden, Verlust verhindern, heikle Bilder löschen)
- Werden Sie zum Handeln gedrängt? («Letzte Mahnung», «Nur noch ganz kurze Zeit» etc.)

! Zu Links

- Versteckt sich hinter dem Link eine völlig andere Website? (Mit Cursor über den Link fahren, analog E-Mail-Adresse des Absenders)

! Zu Anhängen

- Klicken Sie in verdächtigen Mails nie auf Links oder angehängte Bilder und Dateien.
- Erwarte ich (von diesem Absender) Dokumente oder Dateien?
- Handelt es sich um einen potenziell gefährlichen Dateityp? (Nur Endungen mit «.txt» sind immer sicher.)