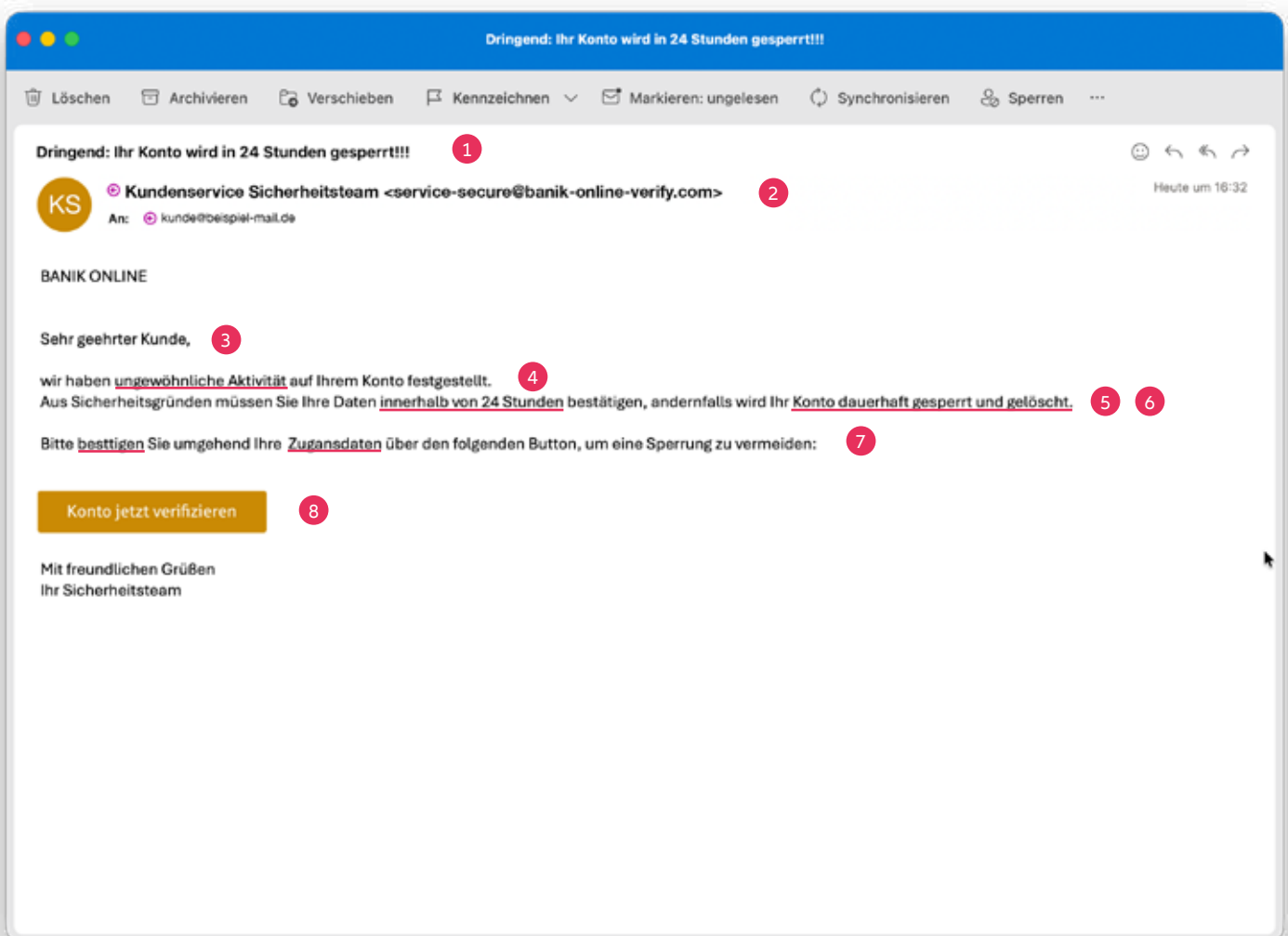


So erkennen Sie eine gefährliche Phishing-Mail

Beispiel-E-Mail mit Erklärungen

Unten sehen Sie eine nachgebaute Beispiel-E-Mail mit acht typischen Warnsignalen. Unterhalb der Beispiel-E-Mail werden diese 8 Warnsignale erklärt.



1 Reißerischer Betreff mit Alarmstimmung

Ausrufezeichen und Wörter wie "dringend" oder "sofort" sollen Panik erzeugen, damit man nicht mehr nachdenkt, bevor man klickt.

2 Absenderadresse passt nicht zur Marke

Der angezeigte Name klingt vertrauenswürdig, aber die eigentliche E-Mail-Adresse stammt von einer fremden Domain. Immer die volle Adresse prüfen, nicht nur den Anzeigenamen.

3

Unpersönliche Anrede

Echte Anbieter sprechen dich meist mit deinem Namen an. Eine generische Anrede wie "Sehr geehrter Kunde" ist ein Hinweis auf eine Massen-Mail.

4

Vage Bedrohungsbehauptung

Es wird von "ungewöhnlicher Aktivität" gesprochen, ohne konkrete Details zu nennen. Das erzeugt Unsicherheit, ohne dass man es prüfen kann.

5

Künstlicher Zeitdruck

Eine kurze, enge Frist soll verhindern, dass du in Ruhe nachdenkst oder die Mail über einen anderen Kanal verifizierst.

6

Drohung mit harten Konsequenzen

Die Androhung von Kontosperrung oder -löschung soll starke Angst auslösen und zu einer unüberlegten Reaktion verleiten.

7

Rechtschreib- und Grammatikfehler

"besttigen" und "Zugansdaten" sind typische Tippfehler. Seriöse Unternehmen lassen ihre Mails professionell Korrektur lesen.

8

Abweichende Linkadresse

Der sichtbare Linktext zeigt eine plausible Adresse, das tatsächliche Ziel ist aber eine völlig andere Domain. Vor dem Klicken immer den echten Link prüfen.

Wichtig:

Diese E-Mail ist frei erfunden und dient nur zu Schulungszwecken. Firmenname, Absender und Links sind fiktiv. Im Zweifel gilt: bei verdächtigen Mails keine Links anklicken, keine Anhänge öffnen und den Absender über einen bekannten, offiziellen Kanal verifizieren.