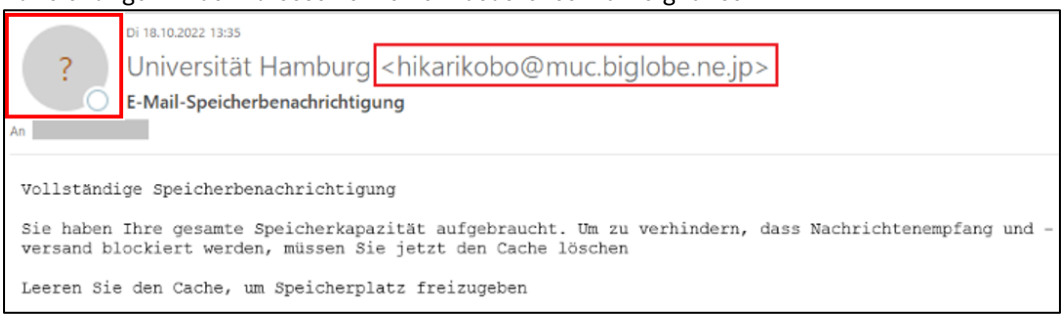
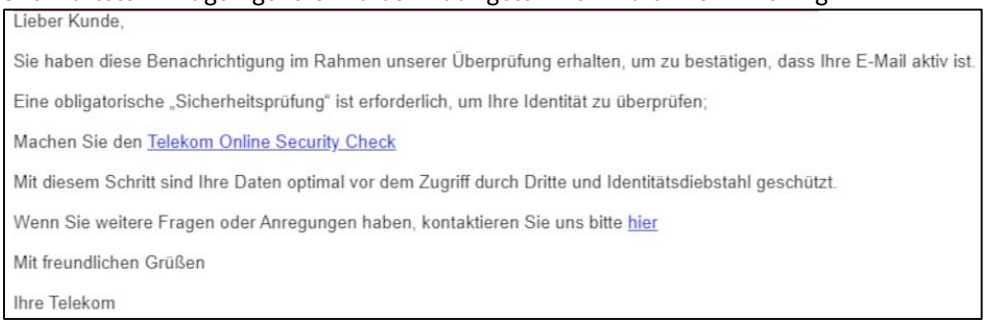
10 Tipps gegen Phishing-Attacken

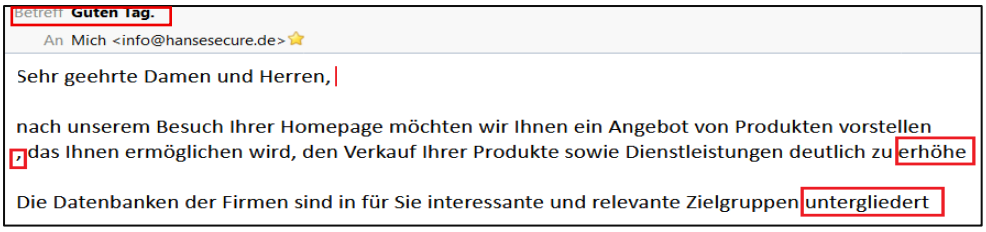
1. Überprüfen der Absenderadresse
   Kontrollieren Sie vor jeder Reaktion die vollständige E-Mail-Adresse des Absenders. Gerade in Hotels werden Phishing-Mails häufig so gestaltet, als stammten sie von Gästen, Buchungsportalen, Lieferanten, Reiseveranstaltern oder internen Ansprechpartnern. Schon kleine Abweichungen in der Adresse können ein deutliches Warnsignal sein.



2. Unerwartete Anfragen grundsätzlich hinterfragen
   Seien Sie besonders vorsichtig bei Nachrichten, mit denen Sie nicht gerechnet haben. Das gilt vor allem bei Anfragen zu Zahlungsdaten, Rechnungen, Reservierungen, Zugangsdaten, Bankverbindungen oder personenbezogenen Informationen von Gästen und Mitarbeitenden. Unerwartete Anfragen gehören zu den häufigsten Merkmalen von Phishing.

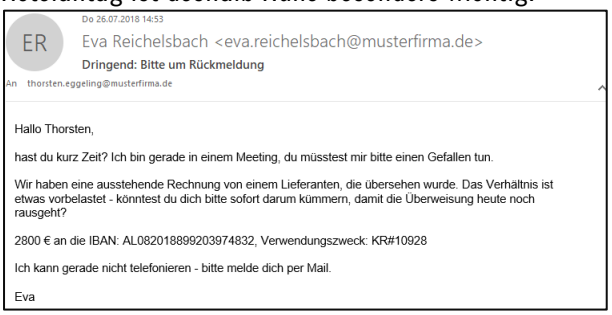


3. Auf Sprache (Grammatik/ Rechtschreibung), Anrede und Stil achten
   Viele Phishing-Mails fallen durch unübliche Formulierungen, Grammatik- oder Rechtschreibfehler sowie eine unpassende Anrede auf. Wenn in Ihrem Haus normalerweise ein bestimmter Ton üblich ist und eine Nachricht davon deutlich abweicht, kann das ein Hinweis auf einen Betrugsversuch sein.



4. Dringende Handlungsaufforderung
   Phishing arbeitet oft mit Zeitdruck, Dringlichkeit oder subtilen Drohungen. Formulierungen wie

„sofort handeln“, „letzte Mahnung“, „umgehend bestätigen“ oder „sonst entstehen Nachteile“ sollen dazu verleiten, unüberlegt zu klicken oder Daten preiszugeben. Gerade im hektischen Hotelalltag ist deshalb Ruhe besonders wichtig.



5. Links Überprüfen
   Klicken Sie nicht direkt auf Links in verdächtigen E-Mails. Prüfen Sie zunächst die Zieladresse, indem Sie mit der Maus über den Link fahren. Besonders gefährlich sind täuschend echte Internetadressen mit kleinen Schreibabweichungen oder Links ohne nachvollziehbaren Zusammenhang zum Inhalt der Nachricht. (Hovern)

6. Anhänge überprüfen
   Öffnen Sie keine Anhänge, wenn Sie diese nicht erwarten oder der Absender unbekannt ist. In Bezug auf Hotels betrifft das häufig vermeintliche Rechnungen, Reservierungsbestätigungen, Bewerbungsunterlagen, Stornierungen oder Zahlungsbelege. Vor dem Öffnen sollte immer geprüft werden, ob Datei, Anlass und Absender tatsächlich zusammenpassen.

7. Betreff, Inhalt und Kontext auf Plausibilität prüfen
   Achten Sie darauf, ob Betreffzeile und Inhalt logisch zusammenpassen. Werden Sie zu einem Vorgang angeschrieben, den Sie nicht kennen? Gibt die Nachricht vor, eine Antwort auf eine E-Mail zu sein, die Sie nie versendet haben? Passen Inhalt, Zeitpunkt und Anliegen überhaupt zum laufenden Hotelbetrieb? Diese Plausibilitätsprüfung ist ein zentraler Schutzmechanismus.

8. Geschäftsbeziehung und Zuständigkeit prüfen
   Fragen Sie sich: Kennen wir den Absender überhaupt? Besteht eine reale Geschäftsbeziehung? Gehört die Anfrage zu meinem Aufgabenbereich? Wenn eine Nachricht keinen Bezug zu Ihrem

beruflichen Zuständigkeitsbereich oder zum Hotelbetrieb hat, ist besondere Vorsicht geboten.

9. Im Zweifel nicht reagieren, sondern intern rückversichern
   Wenn Sie Zweifel an einer Nachricht haben, klicken Sie nicht, öffnen Sie nichts und geben Sie keine Daten weiter. Klären Sie den Vorgang stattdessen über einen bekannten und sicheren Kanal, etwa telefonisch beim tatsächlichen Ansprechpartner oder intern mit der zuständigen IT-Abteilung.

10. Sperren Sie Ihren Arbeitsplatz
    Sperren Sie Ihren PC beim Verlassen des Raumes So verhindern Sie, dass Dritte Zugriff auf Ihre Daten bekommen. (Win+L)