Sechs Tipps gegen Phishing: So haben betrügerische Mails keine Chance

- Es gibt immer mehr „Phishing-Mails“, mit denen Kriminelle versuchen an Daten und Passwörter zu gelangen – und sie sind immer schwerer von seriösen Mails zu unterscheiden
- ING-Expertin Alexandra Schiefer erklärt, woran man betrügerische E-Mails erkennt und wie man sich schützt

Frankfurt am Main, 19.03. 2021: Nur mal kurz die Mails checken – doch dann der Schreck: „Achtung, wir haben eine Unregelmäßigkeit in Ihrem Konto entdeckt“, heißt es in einer der Nachrichten. Hilfe gegen das vermeintliche Problem verspricht der angefügte Link – schnell geklickt und dort die Kundendaten eingegeben. Doch Vorsicht: Was im ersten Moment wie guter Service wirkt, entpuppt sich häufig als Hackerangriff, auch „Phishing“ genannt.

„Phishing“ ist ein Begriff aus der IT, der sich vom Englischen „password fishing“ ableitet: Mithilfe von gefälschten E-Mails oder Websites „angeln“ sich Kriminelle persönliche Daten wie Passwörter oder Kreditkartennummern. Die Mails und Webseiten wirken oft täuschend echt, sodass selbst erfahrene Internetnutzerinnen – und nutzer nicht auf den ersten Blick erkennen können, ob es sich um Betrug handelt. Alexandra Schiefer, Leiterin Betrugsprävention bei der ING Deutschland, gibt sieben Tipps, wie man Phishing erkennt und sich schützt:

1. Achtung bei Gewinnen, Kontoproblemen und Abfrage von Daten

Ihre Kundendaten werden abgefragt? Sie sollen sich über einen Link einloggen, weil es Probleme mit Ihrem Konto gibt? Oder Sie haben etwas gewonnen? Vorsicht! Was erstmal verlockend wirkt, stellt sich häufig als Phishing-Angriff heraus. Auch großartige Rabatte, kostenfreie Programm-Downloads oder die Aufforderung, Kundendaten zu verifizieren, verfolgen nicht selten den Zweck, Sie zu schnellen und unüberlegten Handlungen zu verleiten.

2. Kosten- und Zeitdruck sind verräterisch

Phishing-Mails versuchen typischerweise, Sie unter Handlungsdruck zu setzen: Zum Beispiel mit der Androhung, Ihr Konto werde gesperrt, wenn Sie nichts unternähmen. Oft kombinieren Kriminelle diese Drohung mit Zeitdruck. Typisch sind Aufforderungen wie „Sie müssten

innerhalb von 24 Stunden reagieren.“ Auch Kostendruck ist ein beliebtes Mittel, um Druck aufzubauen, nach dem Motto: „Handeln Sie zu spät, kommt eine Gebühr auf Sie zu.“

3. Auf das eigene Bauchgefühl hören

Die Mail kommt Ihnen merkwürdig vor, und in Ihrer Magengegend macht sich ein mulmiges Gefühl breit – zum Beispiel, weil der Text Rechtschreibfehler hat oder die Absenderadresse unseriös wirkt? Hören Sie auf dieses Warnzeichen! „Die eigene Verunsicherung ist in Sachen Phishing-Mails ein guter Berater“, sagt Alexandra Schiefer. „Behauptungen, wie ein möglicher Missbrauch Ihrer Kreditkarte oder Ihr Konto weise ein erhöhtes Risiko auf, sollen Sie nur zum schnellen, unreflektierten Handeln verleiten.“

4. Keine Links anklicken und Konten selbst im Blick behalten

Klicken Sie nicht auf einen Link in einer Nachricht, der Sie auffordert, Passwörter und Daten auf einer Website zu aktualisieren. Sicherer ist es, die URL, also die Internetadresse, selbst von Hand in den Browser einzugeben. Dies gilt übrigens generell, wenn Sie die Webseite Ihrer Bank aufrufen wollen. Zudem sollten Sie Ihr Konto im Blick behalten und es regelmäßig auf ungewöhnliche Aktivitäten hin überprüfen.

5. Phishing erfolgt über viele Kanäle

Wer glaubt, Phishing erfolge nur per E-Mail, der irrt. Betrugsversuche über SMS, WhatsApp und andere Messenger-Dienste, Briefe und sogar per Telefon sind nicht minder verbreitet. Darum halten Sie sich generell daran, wenn Sie kontaktiert werden: Teilen Sie über diese Kanäle niemals Ihre Passwörter oder Zugangsdaten mit.

6. Informieren Sie sich direkt auf der Website des vermeintlichen E-Mail-Absenders

Wenn Sie eine Phishing-Mail identifizieren: Markieren Sie diese als Spam. Bei Unsicherheiten informieren Sie sich in aller Ruhe auf der Internetseite des betroffenen Unternehmens, ob Ihrerseits Handlungsbedarf besteht. Ein Anruf beim Kundenservice des jeweiligen Anbieters kann ebenso hilfreich sein. So erfahren Sie, ob beispielsweise tatsächlich ein Problem mit Ihrem Kundenkonto besteht. Wichtig: Suchen Sie sich die Telefonnummer des Unternehmens selbstständig heraus und nutzen keine in der Mail aufgeführte Nummern. Die

Verbraucherzentrale veröffentlicht zudem laufend Betrugsfälle auf ihrem Phishing-Radar unter www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar .

Das ING-Sicherheitsversprechen

Die ING Deutschland verspricht ihren Kundinnen und Kunden, finanzielle Schäden zu ersetzen, die durch Missbrauch von Zugangsdaten unter Verwendung des ING-Namens entstehen. Hierfür müssen Kundinnen und Kunden die Bank sofort informieren und parallel Strafanzeige bei der Polizei wegen missbräuchlicher Verwendung der Zugangsdaten erstatten.

Wer sich weiterführend rund um Phishing und Online-Sicherheitsaspekte informieren möchte, findet im ING-Blog „WissensWert“ weitere Hinweise: www.ing.de/wissen/sicherheit/

Sollten Sie künftig keine Verbraucherinformationen mehr von uns wünschen, genügt ein kurzer Hinweis an: presse@ing.de

Medienkontakt

ING Deutschland

Sebastian Göb

Tel.: +49 (0) 152 38927131

E-Mail: Sebastian.goeb@ing.de

Die ING in Deutschland

Mit über 9,5 Millionen Kundinnen und Kunden sind wir die drittgrößte Bank in Deutschland. Unsere Kernprodukte sind Girokonten, Baufinanzierungen, Spargelder, Verbraucherkredite und Wertpapiere. Bei der Kreditvergabe an kleine und mittlere Firmen arbeiten wir im Geschäftskundensegment Business Banking mit der Online-Plattform Lendico zusammen. Im Bereich Wholesale Banking bieten wir Bankdienstleistungen für große, internationale

Unternehmen an. Mit über 6.000 Kolleginnen und Kollegen sind wir in Frankfurt am Main (Hauptquartier), Berlin, Hannover, Nürnberg und Wien vertreten