



Schützen Sie sich vor Phishing

In der täglichen E-Mail-Flut werden auch Sie hin und wieder Phishingmails erhalten. Wenn Sie diese drei Grundregeln im Umgang mit betrügerischen Mails und SMS beachten, können Sie das Risiko für einen Schaden vermindern.

zlb.ch

Häufung von Phishing-Angriffen mit gefälschten E-Banking-Portalen

In jüngster Vergangenheit gab es bei diversen Schweizer Banken vermehrt Phishing-Angriffe. Hierbei werden Kundinnen und Kunden auf die gefälschten E-Banking-Portale geführt. Bei einer Anmeldung auf einem gefälschten E-Banking-Portal können Cyberkriminelle den Benutzernamen und das Passwort abfangen. In einem zweiten Schritt erhalten Kundinnen / Kunden wie bei der gewöhnlichen Anmeldung eine Nachricht auf ihre Multi-Faktor-Authentifizierung (MFA) App auf dem Smartphone und laufen Gefahr, diese zu bestätigen und so den Angreifern Zugang zum E-Banking zu gewähren.

Ob Phishing per E-Mail, Smishing per SMS oder Vishing per Telefon, eines ist sicher, die Herangehensweise der Betrüger wird immer raffinierter. Wenn Sie folgende drei Regeln beachten, sollten Ihre sensiblen Daten vor unbefugtem Zugriff geschützt sein.

Regel 1:

Misstrauen Sie jeder E-Mail oder SMS, die Sie unaufgefordert erhalten

Sollten Ihnen Inhalte oder Absender verdächtig vorkommen, löschen Sie diese umgehend und kontaktieren Sie den Absender über Ihnen bekannte Kontaktmöglichkeiten am besten telefonisch.

Klicken Sie niemals auf einen Link oder eine angehängte Datei, wenn Sie unsicher über die Herkunft sind. Vor allem bei angeblicher Dringlichkeit sollten Sie besonders vorsichtig sein!

Regel 2:

Teilen Sie Passwörter und andere sensible Daten (Kreditkartendaten) niemals mit

Immer wenn es um finanzielle Angelegenheiten geht, sollten Sie besonders misstrauisch sein. **Geben Sie nie Passwörter, Bankkonto-, Kreditkarteninformationen und SMS-Codes weiter und loggen sich nie über eine Landingpage ein, auf die Sie über einen Link in einer E-Mail oder SMS gelangt sind.** Rufen Sie stattdessen die Seite manuell mit Eingabe der Ihnen bekannten Internetadresse auf, falls Sie sich in diesem Moment Zugriff zu diesem Konto verschaffen wollen.

Regel 3:

Antworten Sie nie auf Phishing oder Smishing

Sollten Sie eine E-Mail oder SMS erhalten und nicht als Phishing oder Smishing erkennen, geben Sie niemals sensible Daten bekannt.

Niemand mit guten Absichten wird Sie auf diesem Weg nach Ihrer Kreditkartennummer und Passwörtern fragen. Sollten Sie es zu spät gemerkt und bereits Angaben gemacht haben, sperren Sie sofort Ihre Karte und kontaktieren Sie die ZLB.

Wechseln Sie zur Sicherheit Ihr E-Banking Passwort oder dasjenige der betroffenen Seite. Sperren Sie nach Kontrolle der möglicherweise erfassten Zahlungen Ihren E-Banking-Vertrag und kontaktieren Ihre/n Kundenberater/in.

Wichtige Tipps für ein sicheres Login:

- Rufen Sie nur sichere Seiten auf, die mit <https://> beginnen, um eine sichere Verbindung zu haben (Schloss-Symbol, richtiger Name der Bank und korrekter Domänen-Name).
- Werfen Sie ein Augenmerk auf untypische Absenderadressen, Schreibfehler und Logos.
- Prüfen Sie nach dem Eingeben der Website (URL) die Web-Adresse nochmals. Wurde sie umgeleitet?
- Tippen Sie die Adresse zum E-Banking manuell in der Adresszeile Ihres Browsers ein.
- Verwenden Sie niemals einen Link oder eine Suchmaschine, um sich anzumelden.
- Beenden Sie die Verbindung bei einem Systemunterbruch oder bei ungewöhnlichen Fehlermeldungen sofort.
- [«eBanking – aber sicher!» \(ebas.ch\)](#)
- [Merkblatt – So schützen Sie sich vor Datendiebstahl \(ebas.ch\)](#)