



Phishing

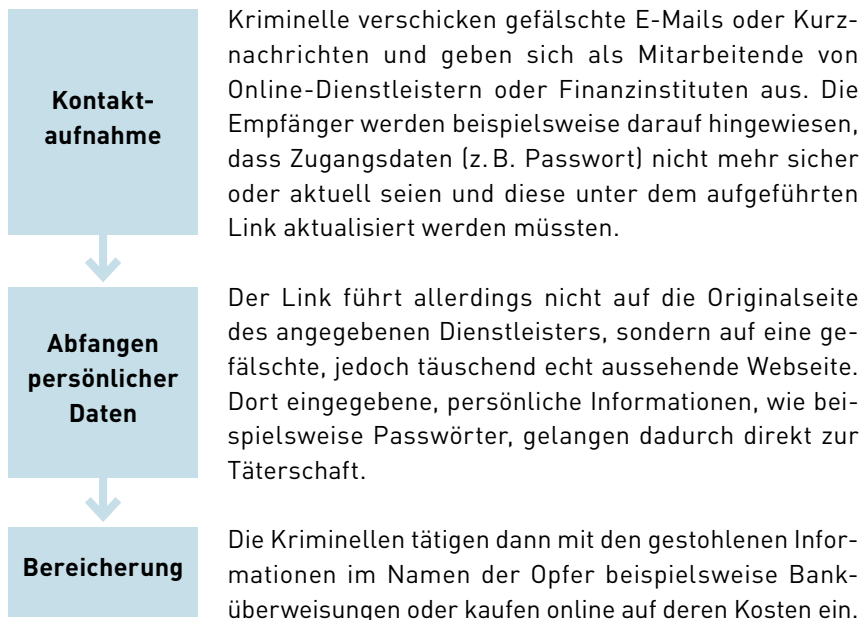
So schützen Sie sich vor Datendiebstahl

Ihre Polizei und die Schweizerische Kriminalprävention (SKP) – eine interkantonale Fachstelle der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), in Zusammenarbeit mit der Hochschule Luzern und «eBanking – aber sicher!»

Wenn ein falscher Klick genügt ...

Phishing ist ein Kunstwort und bedeutet so viel wie «Passwörter fischen». Es geht dabei um den Diebstahl von persönlichen und sensiblen Informationen – in der Regel Passwörter.

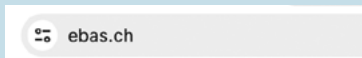
Beim **Phishing** probieren Kriminelle mithilfe von gefälschten E-Mails und Webseiten an Passwörter und andere vertrauliche Informationen, wie z. B. Kreditkartennummern, zu gelangen. Die Angreifer möchten sich mit diesen Informationen finanziell bereichern. Im Visier der Kriminellen stehen meist Anmeldeinformationen für Online-Dienstleister wie Finanzinstitute (E-Banking), Online-Auktionshäuser oder Online-Shops. Auch Kurznachrichten wie SMS, WhatsApp etc. werden immer öfter für Phishing-Angriffe eingesetzt. Das perfide an dieser unter dem Namen **Smishing** (SMS-Phishing) bekannten Phishing-Variante ist, dass die meisten Kriterien zur Erkennung von Phishing-E-Mails bei Kurznachrichten nicht angewandt werden können.



Es gibt auch eine telefonische Variante des Phishing, die nennt man **Vhishing** (von Voice-Phishing). Die Kriminellen geben sich beispielsweise als Polizei oder Finanzinstitut aus und erfinden Geschichten, um an vertrauliche Informationen zu gelangen.

Schützen Sie sich vor Phishing und Smishing, indem Sie

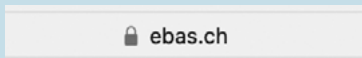
- nie einen Link verwenden, der per E-Mail oder Kurznachricht zugeschickt oder per QR-Code eingescannt wurde, um sich bei einem Online-Dienstleister oder Finanzinstitut anzumelden;
- nie Formulare ausfüllen, die per E-Mail oder Kurznachricht zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern;
- die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben;
- beim Aufruf der Anmeldeseite die TLS-Verbindung (https://, Schlosssymbol, Schieberegler) überprüfen und sich durch die Kontrolle der Internetadresse in der Adresszeile Ihres Browsers vergewissern, dass Sie sich am richtigen Ziel befinden;



Chrome



Firefox



Safari



Edge

- sich bei Unsicherheit oder Unklarheit an Ihren Online-Dienstleister oder Finanzinstitut wenden.

Schützen Sie sich vor Vishing, indem Sie

- vertrauliche Informationen nie einer anderen Person bekannt geben;
- Telefonanrufe, in denen Sie danach gefragt werden, umgehend beenden.

Testen Sie Ihr Phishing-Wissen mit dem Phishing-Quiz von «eBanking – aber sicher!» auf **www.ebas.ch/phishingtest**.

Haben Sie eine Phishing E-Mail, eine Smishing Kurznachricht erhalten oder eine Phishing-Seite gefunden? Melden Sie diese auf **www.antiphishing.ch**.

Weitere Informationen:
www.ebas.ch/phishing
www.skppsc.ch/phishing





Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch

Dieses Faltblatt entstand in Zusammenarbeit mit
der Hochschule Luzern und «eBanking – aber sicher!».

www.ebas.ch | www.ebankingabersicher.ch

HSLU Hochschule
Luzern

eBanking aber sicher!



Juni 2024

