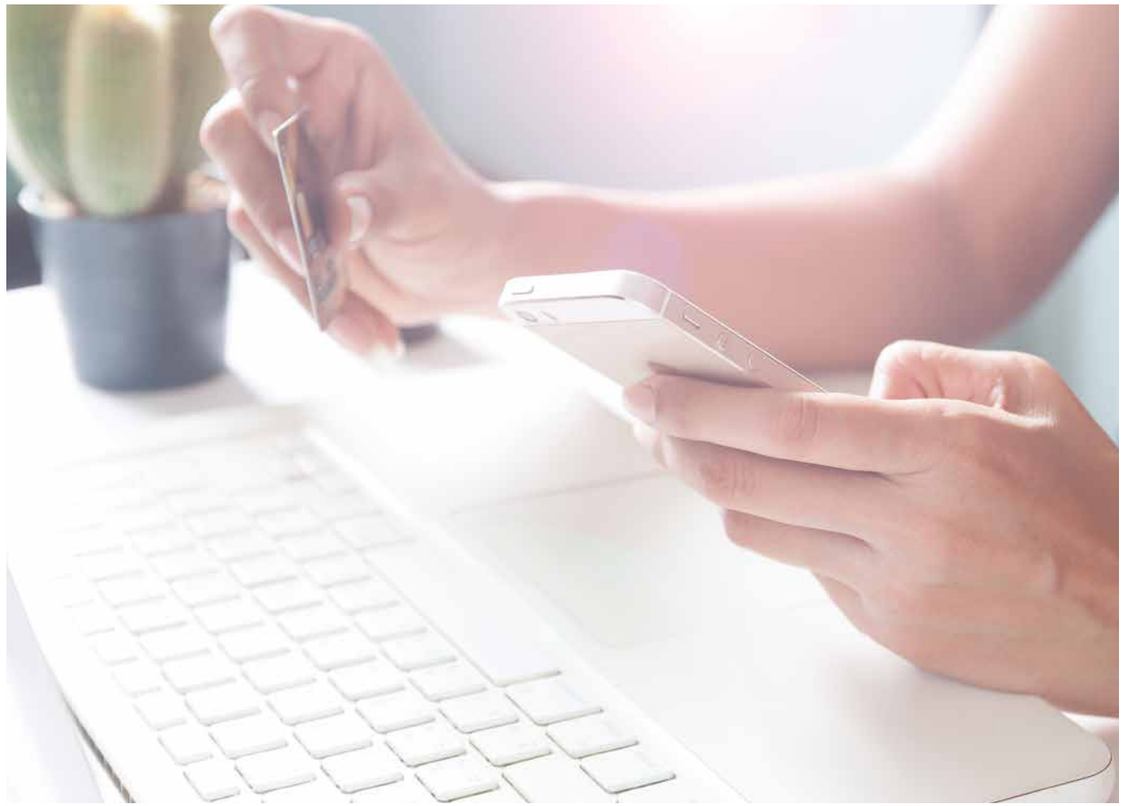
Taschendiebe gibt es auch im Internet

Phishing-Angriffe und bösartige Software bedrohen die Sicherheit des elektronischen Zahlungsverkehrs. Vor Übergriffen schützen Sie sich am wirksamsten mit einer gesunden Portion Misstrauen.

Text **Lara Surber**



Wir kaufen in Onlineshops ein. Unsere Bankgeschäfte erledigen wir via E-Banking. Und stehen wir doch einmal an einer physischen Kasse, können wir unsere Einkäufe mit dem Smartphone bezahlen. Der zunehmend elektronische Zahlungsverkehr ist praktisch, birgt aber auch Risiken. Während in der analogen Welt Taschendiebe und Einbrecher unterwegs sind, haben es Gauner in der digitalen auf Zugangsdaten und Passwörter abgesehen.

Oliver Hirschi, Leiter des Online-Informationsportals «eBanking – aber sicher!» der Hochschule Luzern vergleicht das elektronische Zahlen mit Autofahren. «Eine gewisse Gefahr ist immer da, aber trotzdem machen es alle. Man muss aber die nötigen Sicherheitsvorkehrungen treffen.» Diese Vorkehrungen werden zum einen von den Finanzinstituten vorgegeben. So wird beim E-Banking immer eine sogenannte Zwei-Faktoren-Authentifizierung angewendet: Neben einer Identifikationsnummer und einem Passwort verlangen Banken meist einen weiteren, nur für die aktuelle Sitzung gültigen Sicherheitscode. Zu diesem Zweck wird eine sogenannte Transaktionsnummer (TAN) erzeugt und dem Nutzer übermittelt. Das geschieht beispielsweise mit einer Nachricht an das Smartphone des Nutzers (Mobile TAN oder mTAN) oder indem dieser ein bestimmtes Bild mit dem Smartphone fotografiert (photoTAN). Einige Anbieter generieren den Code für den Zugang ins E-Banking auch mit einem Kartenlesegerät oder versenden Streichlisten an ihre Kunden. Neben diesen ausgeklügelten Sicherheitsbestrebungen von Finanzinstituten ist aber vor allem auch eines entscheidend für den sicheren elektronischen Zahlungsverkehr: das Verhalten der Anwenderinnen und Anwender.

Die Hardware sichern

Das von Hirschi geleitete Informationsportal fasst die wichtigsten Schritte für sicheres E-Banking zusammen. Diese sind auch für den elektronischen Zahlungsverkehr im Allgemeinen gültig. Zunächst geht es darum, die Hardware optimal zu sichern. Installieren Sie dazu ein Virenschutzprogramm und eine Firewall. «Und zwar nach Möglichkeit auf allen Geräten, auch auf dem Tablet und dem Smartphone», so der Experte. Führen Sie regelmässig Software-Updates durch, um mit verbesserten Versionen bestehende Sicherheitslücken zu schliessen. Löschen Sie Apps, die Sie nicht mehr nutzen. Und verwenden Sie sichere Passwörter.

So selbstverständlich diese Tipps scheinen, so häufig werden sie auch missachtet: Gemäss einer Studie des Hasso-Plattner-Instituts war letztes Jahr das meistverwendete Passwort «123456». Wie sicher Ihr Kennwort ist, können Sie auf passwortcheck.ch überprüfen. Auch Bezahl-Apps wie TWINT oder Apple Pay können Sie mit PIN respektive Fingerabdruck sichern. Und gerade wer sein Smartphone zum Bezahlen nutzt, sollte auch das Gerät selbst mit einem Code oder einer Fingerabdruck-Prüfung gegen den Zugriff durch andere schützen. ➤

Der kontaktlose Zahlungsverkehr macht das bargeldlose Zahlen besonders einfach und bequem für den Nutzer.

Misstrauen schützt vor Phishing-Angriffen
Der grösste Gefahrenfaktor im elektronischen Zahlungsverkehr ist gemäss Hirschi aber nicht die Hardware, sondern die Gutgläubigkeit der Nutzerinnen und Nutzer bei sogenannten Phishing-Angriffen. «Da helfen technische Massnahmen nur sehr begrenzt», sagt er. Was hilft, ist gesundes Misstrauen. Phishing – eine Wortmischung aus den englischen Begriffen «Password», «Harvesting» und «Fishing» – bezeichnet den Versuch, auf vertrauliche Informationen anderer zuzugreifen. Als klassisches Phishing gilt der Angriff per Mail. Der Absender versucht mit einer mehr oder weniger glaubwürdigen Geschichte den Empfänger dazu zu bringen, sensible Daten preiszugeben oder Überweisungen zu tätigen. Die Beispiele für Phishing-Mails reichen von sehr einfach zu erkennenden und durchschaubaren Nachrichten bis hin zu solchen mit gefälschten Adressen von vermeintlich seriösen Absendern wie Banken oder Versicherungen – mitsamt korrekt scheinenden Logos, E-Mail- oder Webadressen. Ein typisches Beispiel sind Mails von Paypal zu geänderten AGB. Phishing kann auch telefonisch erfolgen und wird dann auch Vishing (Voice-Phishing) genannt. Auch kann das Opfer mit Malware oder falschen QR-Codes unbemerkt auf eine gefälschte Website geführt, respektive umgeleitet werden. 2016 sind bei der Melde- und Analysestelle Informationssicherung MELANI über 4500 Phishing-Seiten gemeldet worden.

http ist nicht https
Grundsätzlich gilt: Kein seriöser Dienstleister fordert Sie per Mail oder Telefon dazu auf, Passwörter oder Kreditkartendaten anzugeben. Ein weiterer Hinweis auf einen unseriösen Absender sind eine unplausible Mailadresse – auch wenn der Absendername vertrauenswürdig aussieht –, viele Rechtschreibfehler oder eine unpersönliche Anrede. Klicken Sie in verdächtigen Mails nie auf Links und öffnen Sie keine Anhänge, sondern löschen Sie diese umgehend.

Beim Login ins E-Banking sollten Sie sicherstellen, dass Sie sich wirklich auf der Seite Ihrer Bank befinden. In der Adresszeile sollte «https» stehen – ein Zeichen dafür, dass die Daten verschlüsselt übertragen werden – und ein Schlosssymbol sollte angezeigt werden. Beginnen Adressen hingegen mit «http», ist das ein Hinweis auf eine gefälschte Seite. Weiter wichtig: Melden Sie sich nach getaner Arbeit korrekt aus dem E-Banking ab. «Bei der Anmeldung öffnet die Bank eine Tür für Sie. Diese Tür sollten Sie beim Gehen wieder schliessen», erklärt Hirschi. Auch empfiehlt es sich, nach der Onlinesession den Browser-Cache (Speicher) zu leeren. Wer im elektronischen Zahlungsverkehr unvorsichtig ist, dem werden nicht zwingend Daten geklaut – aber falls doch, ist es ärgerlich. Oder wie Hirschi sagt: «Legt man bei der Autofahrt den Sicherheitsgurt nicht an, verletzt man sich deswegen nicht unbedingt. Aber falls doch, trägt man eine Mitschuld.» Und den Grad der Mitschuld überprüfen Finanzdienstleister bei Missbrauchsfällen – genau gleich wie bei Verkehrsunfällen – meist sehr genau. ★

Mehr zum Thema

- Tipps rund um sicheres E-Banking und ein Test zum eigenen Phishing-Wissen gibt es auf der Informationsplattform ebas.ch
- Melden Sie Phishing-Mails auf antiphishing.ch und tragen Sie dazu bei, andere Internetnutzer zu schützen. Bei einigen Webmail-Anbietern geht das ganz einfach per Klick auf einen «Report spam»-Knopf.
- K-Tipp führt eine Liste mit aktuellen Phishing-Fällen: Zur Liste gelangen Sie über diesen QR-Code:

Gewinnen Sie …

… eines von zwei Pflegesets des französischen Kosmetikherstellers FILORGA im Wert von CHF 568.–.

Mit SKIN-ABSOLUTE DAY® und SKIN ABSOLUTE NIGHT® erleben Sie eine ultimative Pflege für mehr Jugendlichkeit. Die Haut wird regeneriert und besticht durch ein pralleres und strahlenderes Aussehen. Sie wird dichter, Falten bilden sich zurück, der Teint wird frischer und gleichmässiger.

In Lichtgeschwindigkeit jünger werden: Die Tagespflege SKIN-ABSOLUTE DAY® des französischen Anti-Aging-Unternehmens beinhaltet das Enzym Extremozyme®, das die UV- und Infrarotstrahlen in Energie umwandelt, und die Photolyase – ein Enzym der Blaualge, wodurch die Kraft des Lichts eingefangen wird. Die Crème ist ebenfalls angereichert mit Hyaluronsäure und dem patentierten Wirkstoffkomplex NCTF®. Die Nachtcrème SKIN ABSOLUTE NIGHT® beinhaltet Meteoritenextrakt sowie eine Braunalge. Parallel dazu glättet und entspannt ein dem Botox ähnlicher Wirkstoff die Gesichtszüge. Ein Kollagenpeptid stimuliert zudem in Verbindung mit Hyaluronsäure die Synthese von Bindegewebsfasern und schenkt der Haut mehr Festigkeit.

FILORGA ist exklusiv bei Marionnaud erhältlich.

Machen Sie mit bei der Verlosung auf:
womeninbusiness.ch/verlosung