auditives
SF Public Relations GmbH

Interview: Online-Banking: Tipps für sichere Bankgeschäfte im Netz.

Interview mit Ildiko Bruhns, ESET Deutschland GmbH

|Anmoderationsvorschlag:|
Rund 73 Prozent aller Internetnutzer erledigen ihre Bankgeschäfte bereits im Netz. Online-Banking ist beliebt und das bei jung und alt in gleichem Maße. Das wissen leider auch die Internetkriminellen und mit immer neuen, fiesen Tricks versuchen sie, die Konten ahnungsloser Opfer leerzuräumen. Ich spreche dazu mit Ildiko Bruhns von ESET Deutschland:

|Begrüßung Moderator/in:|
Guten Tag Frau Bruhns, ich grüße Sie.

|Begrüßung Ildiko Bruhns:| **0:01“**
Hallo, ich grüße Sie!

1. Frage: Welche Vorteile hat Online-Banking? **0:36“**
Ja, Online-Banking ist beliebt und wird auch immer öfter genutzt. Also, Bankgeschäfte mal eben unterwegs auf dem Smartphone abzuwickeln, ist für Nutzer natürlich super bequem. Und wie beim Online-Shopping schätzen sie auch beim Internet-Banking die Vorzüge, ihre Finanzgeschäfte eben dann erledigen zu können, wenn es zeitlich für sie am besten passt. Der Gang in die nächste Bankfilliale, Warteschlangen oder Öffnungszeiten gehören so der Vergangenheit an. Und mit Online-Banking können ja alle möglichen Konten verwaltet werden, vom normalen Girokonto bis hin zum Bauspar-, Tagesgeld- oder Festgeldkonto. Und je nach Bank lassen sich sogar Aktienkäufe tätigen.

2. Frage: Wer nutzt die Möglichkeiten des Online-Bankings? **0:25“**
Im Moment nutzen rund 40 Millionen Deutsche Online-Banking, Tendenz steigend. Und für viele ist es bereits eine Selbstverständlichkeit geworden, ihre Bankgeschäfte online zu erledigen. Und das gilt im übrigen für Jung und Alt, denn am häufigsten regeln mit 83 Prozent die 50- bis 64-jährigen ihre Finanzen im Netz und mehr als die Hälfte der Internetnutzer ab 65 Jahren nutzen sogar die Online-Option.

3. Frage: Welche Trends gibt es beim Online-Banking? **0:17“**
Also, beim Online-Banking geht der Trend ganz klar hin zum Mobile-Banking. Also, mit Smartphones, Tablets oder Banking-Apps lässt sich zum Beispiel der Kontostand überall abrufen, der Dienst ist jederzeit und immer verfügbar. Das entspricht natürlich dem Wunsch von vielen Nutzern nach größtmöglicher Unabhängigkeit.

4. Frage: Welche Gefahren lauern beim Online-Banking im Netz? **0:23“**
Ja, je mehr das Internet genutzt wird, umso mehr steigt die Cyberkriminalität. Das gilt natürlich auch fürs Online-Banking, denn mittlerweile gehört Diebstahl und Missbrauch von Bankdaten und Kreditinformationen zu den häufigsten Straftaten im Netz. Deswegen ist auch das Thema Sicherheit so wichtig. Denn nur wer sich mit wachen Augen und gesundem Menschenverstand durchs Internet bewegt, kann Cyberkriminellen einen Riegel vorschieben.

5. Frage: Worauf sollten Nutzer ganz allgemein beim Online-Banking achten? 0:36“
Es ist eigentlich so, dass jeder mit ein paar Tipps die Sicherheit beim Online-Banking erhöhen kann, auch wenn es scheinbar ganz banale Dinge sind. Also, zum Beispiel sollten sie ihre Zugangsdaten und TANs sicher aufbewahren. Und dann sollten sie ihre Bankdaten niemals ohne weiteres im Internet weitergeben, also schon gar nicht in sozialen Netzwerken oder bei dubiosen Online-Shops. Immer wieder gerne gemacht, aber ein absoluter Grundfehler ist, die Bankdaten auf dem Smartphone zu speichern. Und außerdem sollten die Passwörter für den Zugang zum Online-Banking regelmäßig geändert werden. Und sehr gern vergessen wird auch das Abmelden nach einer Banksession.

6. Frage: Welche Tricks wenden Online-Betrüger an, um an Bankdaten und Kreditinformationen von Internetnutzer zu gelangen? 0:42“
Also, Online-Betrüger haben einige, auch sehr fantasiereiche Methoden entwickelt, um an die Bankdaten der Internetnutzer zu gelangen. Zum Beispiel mit gefälschten Webseiten. Also, zuerst schleusen Cyberkriminelle Trojaner oder eine andere Schadsoftware auf die Geräte der ahnungslosen Nutzer ein. Und dann leiten sie sie so auf manipulierte Webseiten von Bankunternehmen um. Also, solche Webseiten sind auch täuschend echt aufgesetzt und der Nutzer, der erkennt keinen Unterschied, zumal er ja auch glaubt, die richtige URL eingegeben zu haben. Und auf der gefälschten Seite dann werden die Kunden dann aufgefordert, PIN und TAN einzutippen. Und geben die Nutzer dann dort ihre Daten auch ein, haben die Betrüger freie Fahrt und können sich am Bankkonto sofort zu schaffen machen.

7. Frage: Welche Methoden setzen Online-Betrüger noch ein, um die Nutzer beim Online-Banking auszuspionieren? 0:32“
Phishing-Mails sind bei Internetkriminellen auch sehr beliebt, um an die Bankdaten ihrer Opfer zu kommen. Also, solche Mails gehen auch um, wie ein Lauffeuer und stammen angeblich von PayPal oder einer Bank. Und auch hier werden die Nutzer aufgefordert, ihre Daten zu bestätigen. Und diese E-Mails setzen Kunden meistens noch mehr unter Druck, denn sie behaupten, dass sie ohne die Eingabe der Daten keinen Zugriff mehr auf ihr Konto hätten. Also, klicken die Nutzer nun auf einen angegebenen Link und geben dort ihre Daten ein, ist das Leeräumen des Kontos eigentlich nur noch Formsache.

8. Frage: Was unternehmen Cyberkriminelle noch, um an die gewünschten Daten der Nutzer zu kommen? 0:39“
So genannte Keylogger liegen voll im Trend. Also, die zeichnen jeden Tastenanschlag eines infizierten Geräts auf und übermitteln so die Login-Daten an die Hintermänner. Und die warten natürlich auf den richtigen Moment, bevor sie aktiv werden, nämlich: Sobald der Nutzer über den Browser eine reguläre Bank-Webseite oder ein Zahlungsportal aufruft, gleicht der Schädling zunächst die Adresse der Bank mit einer Datenbank ab. So erfährt der Betrüger, dass ab jetzt alle nachfolgenden Eingaben von großem Wert sind. Und das Schadprogramm zeichnet im Anschluss automatisch die Tastatureingaben auf. Und auf diese Weise werden alle wichtigen Daten eben abgefangen und für kriminelle Zwecke missbraucht.

9. Frage: Welche Tipps können Sie den Internetnutzern geben, damit sie ihre Finanzen im Netz besser schützen können? 0:25“
Ja, mein wichtigster Tipp ist: Klicken Sie auf keine Links und Anhänge in E-Mails in angeblichen Bankanschreiben. Also, keine Bank schickt seinen Kunden E-Mails, um Daten bestätigen zu lassen. Das gleiche gilt auch für unaufgeforderte Aufrufe von Banken, vor allen Dingen, wenn man zur Preisgabe von PIN oder Passwort angehalten wird. Auch wenn es alles noch so seriös erscheint, rufen Sie im Zweifel lieber ihre Bank an und schildern Sie den Vorfall.

10. Frage: Worauf sollten Nutzer außerdem achten, damit sie ihre Bankgeschäfte im Internet sicherer machen können? **0:35“**
Achten Sie auf das HTTPS oder dieses Schlosssymbol in der Adresszeile des Browsers. Sichern Sie Ihr WLAN und auch den Router mit einem starken Passwort ab. Viele Nutzer haben das voreingestellte Passwort vom Internetanbieter nie geändert, obwohl die Standard-Anmeldedaten oftmals leichte Beute für Angreifer sind. Halten Sie Ihren Browser und die Software immer topaktuell und regelmäßige Updates von Betriebssystem, Programmen oder vom Browser, sind Pflicht. Und ganz, ganz wichtig: Setzen Sie eine aktuelle Antiviren-Software ein. Am Besten mit einer Firewall und Anti-Spyware gegen Keylogger und Co.

11. Frage: Warum ist eine aktuelle Antiviren-Software so wichtig? **0:28“**
Also, eine aktuelle Antiviren-Software ist auch deshalb so wichtig, weil Online-Betrüger immer raffinierter werden und ständig neue Methoden entwickeln, um ihre Opfer zu täuschen. Also, es gibt immer mehr Banden von Internetkriminellen, die versuchen, über Schadprogramme, wie Viren, Würmer oder Trojaner ans große Geld zu kommen. Unsere Produkte zum Beispiel enthalten neben Spam-Filter auch Anti-Phishing-Module, die gefälschte Webseiten oder gefährliche Anhänge erkennen. Und das macht das Surfen im Netz weitaus sicherer.

12. Frage: Welche Lösungen bietet ESET? **0:25“**
Also, unsere Produkte bieten auf jeden Fall einen starken Malware-Schutz, selbst gegen verschlüsselte Viren & Co. Und sie verfügen über eine Firewall und schützen vor manipulierten E-Mails und Webseiten. Und wir haben eine Extra-Funktion für Bezahlvorgänge im Netz. Das heißt, Finanztransaktionen werden hier über einen abgesicherten Browser abgewickelt und die von der Tastatur an den Browser übermittelten Daten werden noch zusätzlich verschlüsselt.

|Verabschiedung Moderator/in:|
Frau Bruhns, vielen Dank für das Gespräch.

|Verabschiedung Ildiko Bruhns:| **0:02“**
Ich danke Ihnen auch, tschüß.