

Thema: Bankgeschäfte im Netz - Wie sicher ist Online-Banking?

Beitrag: 2:26 Minuten

Anmoderationsvorschlag: Hacker, die Anzeigetafeln und Ticketautomaten der Bahn lahmlegen. Internet-Gangster, die sich Passwörter und Login-Daten angeln, um Konten leerräumen: Nichts und niemand scheint vor den Kriminellen sicher zu sein. Besonders Bankkunden sind jetzt natürlich verunsichert. Sie fragen sich: Wie riskant ist Online-Banking? Das weiß meine Kollegin Helke Michael.

Sprecherin: Die gute Nachricht zuerst: Online-Banking ist weiterhin sicher. Allerdings müssen dafür ein paar einfache Regeln befolgt werden. Denn meistens versuchen die Kriminellen durch sogenanntes Phishing Konten leerräumen. Dazu geben sich die Täter als Bank aus, sagt Ralph-Christoph Arnoldt vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken – kurz BVR.

O-Ton 1 (Ralph-Christoph Arnoldt, 28 Sek.): „Als Kunde wird man dann aufgefordert, seine Daten, wie z.B. Kontonummer und PIN, auf einer nachgeahmten Webseite einzugeben oder zu nennen. So kommen die Kriminellen an Login-Daten und Passwörter und können damit dann im schlimmsten Fall das Konto plündern. Um das zu vermeiden, ist wichtig zu wissen: Ihre Bank fragt Sie niemals nach vertraulichen Informationen, wie Kontodaten oder persönlichen Daten und wird Ihnen auch keine Links zum Online-Banking per E-Mail schicken.“

Sprecherin: Eine andere Methode ist der Einsatz von Schadsoftware. Über Trojaner werden dann die Login-Daten oder Passwörter einfach abgefangen. Deshalb sollten Virens Scanner und Firewall immer auf dem neuesten Stand sein.

O-Ton 2 (Ralph-Christoph Arnoldt, 20 Sek.): „Außerdem gilt es bei eingehenden E-Mails eine gesunde Skepsis zu bewahren: Kunden sollten weder auf dem PC noch auf dem Smartphone Weblinks aus unbekanntem Quellen anklicken und auch keine unbekanntem Anhänge öffnen. Denn dahinter kann sich immer Schadsoftware verbergen.“

Sprecherin: Eine andere Masche der Betrüger ist es, Bankkunden dazu zu bringen, Testüberweisungen durchzuführen.

O-Ton 3 (Ralph-Christoph Arnoldt, 16 Sek.): „Der BVR kann hier für alle Volksbanken Raiffeisenbanken sprechen: Testüberweisungen gibt es nicht. Bankmitarbeiter werden Sie nie auffordern, Geld irgendwohin zu überweisen oder irgendwelche Programme zu installieren. Als Kunde sollte man also immer wachsam sein.“

Sprecherin: Übrigens: Die sicherste Methode für das Online-Banking ist und bleibt der TAN-Generator, der zum Beispiel mit dem neuen Sm@rt-TAN photo Leser benutzt wird.

O-Ton 4 (Ralph-Christoph Arnoldt, 33 Sek.): „Die Nutzung ist denkbar einfach. Die Girocard wird in den TAN-Generator gesteckt und kurz an den PC-Bildschirm gehalten. Über die optische Schnittstelle des Lesers werden dann die Überweisungsdaten an den TAN-Generator übertragen und im Display des Lesers angezeigt. So sieht man immer genau, für welche Transaktion die Transaktionsnummer verwendet wird. Man hat so die Möglichkeit, den Auftrag noch einmal genau zu prüfen, bevor er endgültig ausgeführt wird. Mit dieser bequemen Technik sind die Kunden bei Online-Banking-Geschäften auf der sicheren Seite.“

Abmoderationsvorschlag: Weitere Informationen rund ums Thema „Sicheres Online-Banking“ finden Sie auf der Webseite vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken unter www.bvr.de.

Thema: Bankgeschäfte im Netz - Wie sicher ist Online-Banking?

Interview: 4:55 Minuten

Anmoderationsvorschlag: Hacker, die Anzeigetafeln und Ticketautomaten der Bahn lahmlegen. Internet-Gangster, die sich Passwörter und Login-Daten angeln, um Konten leerzuräumen: Nichts und niemand scheint vor den Kriminellen sicher zu sein. Besonders Bankkunden sind jetzt natürlich verunsichert. Sie fragen sich: Wie riskant ist Online-Banking? Darüber sprechen wir jetzt mit Ralph-Christoph Arnoldt vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), hallo.

Begrüßung: „Schönen guten Tag!“

1. Herr Arnoldt, ist in Zeiten von regelmäßigen Cyber-Attacken das Geld auf dem eigenen Konto noch sicher?

O-Ton 1 (Ralph-Christoph Arnoldt, 25 Sek.): „Ja, Online-Banking ist auf jeden Fall weiterhin sicher. In Deutschland gibt es knapp 60 Millionen Online-Konten und in weniger als 0,01 Prozent der Fälle hatten Cyber-Kriminelle mit einer Phishing-Attacke Erfolg. Die Chance, selbst zum Opfer zu werden, ist also äußerst gering. Dies gilt umso mehr, wenn man ein paar grundlegende Verhaltensweisen beachtet, die aber auch sonst für Transaktionen im Internet gelten.“

2. Worauf genau muss man als Kunde denn achten?

O-Ton 2 (Ralph-Christoph Arnoldt, 43 Sek.): „In der Regel versuchen Kriminelle die Konten durch sogenanntes Phishing leerzuräumen. Das heißt, die Täter schicken fingierte E-Mails an beliebig ausgewählte E-Mail-Adressen oder rufen Sie sogar an und geben sich dabei als Bank aus. Als Kunde wird man dann aufgefordert, seine Daten, wie z.B. Kontonummer und PIN, auf einer nachgeahmten Webseite einzugeben oder zu nennen. So kommen die Kriminellen an Login-Daten und Passwörter und können damit dann im schlimmsten Fall das Konto plündern. Um das zu vermeiden, ist wichtig zu wissen: Ihre Bank fragt Sie niemals nach vertraulichen Informationen, wie Kontodaten oder persönlichen Daten und wird Ihnen auch keine Links zum Online-Banking per E-Mail schicken.“

3. Gibt es denn noch andere Wege, wie Kriminelle versuchen an unser Geld zu kommen?

O-Ton 3 (Ralph-Christoph Arnoldt, 51 Sek.): „Eine andere Methode der Kriminellen ist der Einsatz von Schadsoftware, um so auf das Konto des Kunden zugreifen zu können. Mit diesen sogenannten Trojanern können direkt auf dem Computer Login-Daten und Passwörter abgefangen werden. Als Kunde kann ich mich aber auch davor einfach schützen, indem ich immer meine Sicherheitssoftware, wie Virens Scanner oder Firewall, auf dem aktuellsten Stand halte. Also installieren Sie immer regelmäßig die vom Anbieter bereitgestellten Updates. Außerdem gilt es bei eingehenden E-Mails eine gesunde Skepsis zu bewahren: Kunden sollten weder auf dem PC noch auf dem Smartphone Weblinks aus unbekanntem Quellen anklicken und auch keine unbekanntem Anhänge öffnen. Denn dahinter kann sich immer Schadsoftware verbergen.“

4. Wer Online-Banking macht, weiß, dass dafür Transaktionsnummern – kurz TAN genannt – genutzt werden. Sind diese denn wenigstens sicher?

O-Ton 4 (Ralph-Christoph Arnoldt, 47 Sek.): „Die Kriminellen sind natürlich sehr kreativ und passen ihre Methoden laufend an. Aber die modernen TAN-Verfahren der Banken sind bei richtiger Anwendung sehr sicher. Mittlerweile haben die Kriminellen aber auch hier Wege gefunden, um Bankkunden zu schädigen. Ein Beispiel: Betrüger versuchen mittels E-Mail den Kunden zu überreden, ungewollte Transaktionen auszuführen, also zum Beispiel sogenannte Testüberweisungen oder Rücküberweisungen für angeblich zu viel auf ihrem Konto eingegangenes Geld. Der BVR kann hier für alle Volksbanken Raiffeisenbanken sprechen: Testüberweisungen gibt es nicht. Bankmitarbeiter werden Sie nie auffordern, Geld irgendwohin zu überweisen oder irgendwelche Programme zu installieren. Als Kunde sollte man also immer wachsam sein.“

5. Wie kann man sich denn vor dem Missbrauch der TAN schützen?

O-Ton 5 (Ralph-Christoph Arnoldt, 62 Sek.): „Das Wichtigste für den Kunden ist, stets auf das jeweilige Gerät, das für Online-Banking genutzt wird, zu achten. Das ist häufig ja das Smartphone, das für mobileTAN oder ein App-basiertes TAN-Verfahren registriert ist. Auch da sollten die üblichen Virens Scanner installiert werden, um sich vor einem Auslesen der Daten zu schützen. Die sicherste Methode für das Online-Banking ist und bleibt jedoch der TAN-Generator, der zum Beispiel mit einem der neuen Sm@rt-TAN photo Leser benutzt wird. Die Nutzung ist denkbar einfach. Die Girocard wird in den TAN-Generator gesteckt und kurz an den PC-Bildschirm gehalten. Über die optische Schnittstelle des Lesers werden dann die Überweisungsdaten an den TAN-Generator übertragen und im Display des Lesers angezeigt. So sieht man immer genau, für welche Transaktion die Transaktionsnummer verwendet wird. Man hat so die Möglichkeit, den Auftrag noch einmal genau zu prüfen, bevor er endgültig ausgeführt wird. Mit dieser bequemen Technik sind die Kunden bei Online-Banking-Geschäften auf der sicheren Seite.“

Ralph-Christoph Arnoldt vom BVR über sicheres Online-Banking. Vielen Dank für das Gespräch!

Verabschiedung: „Ich danke Ihnen!“

Abmoderationsvorschlag: Weitere Informationen rund ums Thema „Sicheres Online-Banking“ finden Sie auf der Webseite vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken unter www.bvr.de.