

Die E-Kriminalität wird immer dreister



Maximilian Reimann

Online-Finanzdienstleistungen per Internet, Bancomaten und Kreditkarten sind hervorragende Einrichtungen im Finanz- und Zahlungsverkehr, haben aber auch ihre Gefahren. Deshalb lieber Vorsicht über alles, als das Nachsehen haben.

Bald am Laufmeter erhalte ich, wie wohl auch ein grosser Teil der Leserschaft, von irgendwelchen Absendern die Aufforderung, den Sicherheitszugang zu bestimmten Online-Finanzdienstleistern zu überprüfen und dann zu aktualisieren. Häufig strotzt der Text gar noch von Sprachfehlern und stinkt somit erst recht zum Himmel. Und ganz besonders, wenn ich die Online-Beziehung zu einer Bank überprüfen soll, bei der ich überhaupt kein Konto habe...

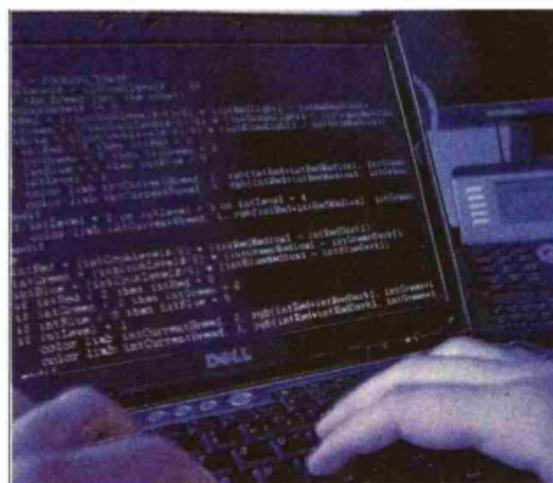
Post mit grösster

Online-Finanzkundschaft

Kommt die Aufforderung aber vermeintlich von der PostFinance und ist sie ohne Fehl und Tadel abgefasst, dann könnte sie vom einen oder anderen der rund 1,5 Millionen Online-Kunden vielleicht doch ernst genommen werden. Mit dieser Kundenzahl

ist PostFinance bekanntlich ganz klar die Nummer 1 im Schweizer Online-Banking. Natürlich bin auch ich einer von ihnen und bei mir ist am 6. Februar folgendes Mail eingegangen:

«Bitte beachten Sie, dass der PostFinance Online-Zugriff auf Ihr Konto in Kürze abläuft. Um Ihre vorhandene E-Finance zu aktualisieren, benutzen Sie bitte den Link... » Es folgte eine auf den ersten Blick recht glaubwürdige e-Finance-Adresse mit «secure»- und «upgrade»-Hinweisen. Natürlich, jeder auch nur einigermaßen



Vorsicht mit fingierten E-Mails. Foto: zVg
vernünftige Postkunde verschiebt das Mail umgehend in den Papierkorb und sperrt den Absender. Wer hingegen die e-Adresse anklickt und sei es nur aus Neugier, könnte den anonymen Internet-Kriminellen schon auf den Leim gehen und ihnen damit den Zugang zum eigenen Konto oder Depot erleichtern. Deshalb absolut Finger weg vor solchen Aufforderungen, woher sie immer auch kommen. Weder Banken, noch PostFinance noch irgendwelche anderen Finanzunternehmen würden je ihre Kundschaft

auf diese anonyme Art und Weise aufordern, irgendwelche Eingaben zur Nachrüstung ihres persönlichen Online-Zugangs zu machen.

Zahl- und Kreditkarten-Betrügereien weiter zunehmend

Ein anderes Kapitel sind die immer raffinierter werdenden Tricks, um an die Daten von Kartenbenutzern heranzukommen. Abgenommen hat allerdings die Zahl der Bancomat-Manipulationen, denn hier sind der Abwehrkampf intensiviert und die Gegenmassnahmen ebenfalls ingenieurer geworden. Dafür haben die Skimming-Fälle, wie diese Kartenbetrügereien in der Fachsprache genannt werden, in Shoppingzentren, Detailhandelsläden und an Tankstellen zugenommen. So sind beispielsweise im letzten Dezember die Kartenlesegeräte in den Migros-Filialen von Sisach und Oberwil manipuliert worden, wie es den Anschein macht, durch die gleiche Täterschaft. Diese liess sich vermutlich über Nacht in der Lokalität einschliessen und hatte dann alle Zeit, um Skimming zu betreiben, d.h. an den Kartenlesern Vorrichtungen anzubringen, um dann die Magnetstreifendaten kopieren zu können. Umgehend nach Aufdeckung der Fälle sind die manipulierten Geräte ausgewechselt worden.

Empfehlungen der Polizei

Angesichts der misslichen Lage ist die Polizei nicht untätig geblieben. Letztes Jahr hat sie auf Ebene Bund und Kantone sowie in Zusammenarbeit mit der Bankiervereinigung die landesweite Präventionskampagne

«Stop Skimming» lanciert. Wer sich näher dafür interessiert, klicke im Internet die Webseite www.stop-skimming.ch an. Man erfährt da die aktuell häufigsten Tricks, wie die meist bandenmässig operierende Täterschaft vorgeht, sowie die wirksamsten Massnahmen, wie man sich individuell am besten dagegen schützt. Diese reichen von der Wahl des Pin-Codes, dessen Eingabe an den Zahlterminals, zu den Ablenkungsmanövern an Bancomaten wie beim bargeldlosen Bezahlen, Tipps für die Geschäftsinhaber, bis hin zur regelmässigen genauen Kontrolle des eigenen Kontostandes. Und ein ganz wichtiger Tipp zum Schluss: Sich nie bei allfälligen Problemen von fremden Personen helfen lassen, sowie die Karte lieber einmal zu viel als einmal zu wenig sperren lassen! Ein weiteres Kapitel, auf das ich hier nicht weiter eingehe, sind die ebenfalls zunehmend dreisten Anrufe per Telefon.