«Phishing» – Tricktäuschung in Wort und Schrift

Die Bank EKI wird Sie nie in einem unangeforderten E-Mail, Telefongespräch oder einer Kurznachricht darum bitten, vertrauliche Personendaten bekannt zu geben. Hüten Sie sich vor «Phishing». Dieser Diebstahl von persönlichen Daten wurde in letzter Zeit in den Medien ausführlich behandelt. Viele Verbraucher und Investoren fürchten um die Geheimhaltung ihrer persönlichen Daten - mit diesem Beitrag will die Bank EKI über das Thema aufklären:

«Phishing» ist eine Art Betrug über vermeintlich seriöse E-Mails, Instant Messages und Webseiten, um Personen ihre vertraulichen persönlichen Daten zu entlocken. Der Begriff stammt von «fishing», dem Angeln ab. Das eingesetzte «ph» steht für «password harvesting» (Passwort ernten). Die Betroffenen sollen durch eine Täuschung persönliche Daten preisgeben, welche einen Kreditkartenbetrug und andere gravierende Eingriffe in ihre Privatsphäre ermöglichen.

Gefälschte E-Mails, welche den Mails seriöser Unternehmen täuschend ähnlich sehen, fordern den Empfänger auf, per Antwort-Mail oder auf einer Webpage seine persönlichen Daten zu aktualisieren. Die unechten E-Mails enthalten manchmal das Logo des Unternehmens und sogar eine Adresse.

Meist wird die Angabe folgender Daten verlangt: Name und Adresse des Benutzers; Sozialversicherungsnummer (beispielsweise AHV-Nummer); Kontonummern und Kennwörter; Bankkonto- und Kreditkartenangaben – manchmal sogar der Mädchenname des Kontoinhabers oder andere private Informationen, welche zu gemeinhin zu Sicherheitszwecken verwendet werden.

Ansprechpartner

Wenn Sie glauben, dass der Name und/oder der Ruf von der Bank EKI in betrügerischer Absicht missbraucht wurden, leiten Sie das Phishing-E-Mail bitte unverändert an info@bankeki.ch weiter. Bitte stellen Sie sicher, dass dieses E-Mail keine sensitiven persönlichen Daten wie Kontoangaben enthält.

Schützen Sie sich

Folgende Massnahmen können Sie selber treffen, damit Sie nicht in die «Phishing»-Falle tappen:

- Seien Sie wachsam, wenn Sie unerwartete E-Mails, Instant Messages, Voicemails oder Faxsendungen erhalten, welche vorgeben, von Ihrer Bank, Ihrem Kreditkartenunternehmen oder Ihrem Online-Broker zu stammen. Falls Ihnen solche Nachrichten zukommen, setzen Sie sich am besten zuerst mit dem Kundendienst Ihrer Bank, Ihres Kreditkartenunternehmens oder Ihres Online-Brokers in Verbindung, um abzuklären, ob die Nachricht echt ist. Entsprechende Kontaktangaben finden Sie auf Ihren jeweiligen Kontoauszügen. Benutzen Sie auf keinen Fall die Verbindungswege, die in der verdächtigen Nachricht aufgeführt werden.
- Beantworten Sie keine E-Mails, Telefonate oder Telefaxe, welche Sie veranlassen, Ihre persönlichen Daten preiszugeben.
- Klicken Sie keine Links in verdächtigen E-Mails an. Dies könnte zur Folge haben, dass automatisch «Spyware» (Spionagesoftware) oder «Keylogger» (Tastaturrekorder) auf Ihren Computer geladen werden.
- Loggen Sie sich regelmässig in Ihre Online-Konten (Bankverbindung, Kreditkarte, Debitkarte oder andere) ein, um den aktuellen Kontostand und alle Transaktionen auf ihre Richtigkeit zu überprüfen. Gleichzeitig sollten Sie auch regelmässig Ihre Kontoauszüge auf unberechtigte Belastungen kontrollieren.
- Benutzen Sie aktuelle Antiviren-Software.
- Spam-Filter und sogar «Anti-Phishing»-Software sind erhältlich, um potenzielle «Phisher» auf Webseiten und in E-Mails automatisch auszublenden.

Bitte merken Sie sich, dass die Bank EKI Sie nie in einem E-Mail, Telefongespräch oder einer Kurznachricht darum bitten wird, vertrauliche Personendaten bekannt zu geben, ohne von Ihnen dazu aufgefordert worden zu sein.

Aktualisiert: 1.12.2014