Schutz vor Phishing

Zehn Goldene Regeln zum Schutz vor Phishing
Die Experten der Bundeskammer der Architekten und Ingenieurkonsulenten haben einen Katalog von zehn Grundregeln vorgestellt, deren Beachtung und vor allem Einhaltung vor Phishing schützt.

1. Nutzung vertrauenswürdiger Computer: „Vergewissern Sie sich, dass nur Personen Ihres Vertrauens das Computersystem nutzen oder administrieren. Wickeln Sie niemals Bankgeschäfte über nicht vertrauenswürdige Computer ab."

2. Verwendung sicherheitsoptimierter Betriebssysteme: „Nur gepflegte und gewartete Computersysteme sind gute Computersysteme - das Betriebssystem muss in regelmäßigen Abständen mit den neuesten Erweiterungen der Sicherheitssoftware (Patches) versorgt werden. Aktivieren Sie die automatischen Updates und den Phishing-Filter im Internet-Browser."

3. Einsatz von Virenschutz und Firewall: „Verwenden Sie ein State-of-the-art Virenschutzprogramm mit automatischen Updates von Virensignaturen gegen Spyware, Viren und Trojaner. Installieren bzw. aktivieren Sie eine Firewall zum Schutz Ihres Computersystems."

4. Vertraulichkeit von PIN und TAN: „Geben Sie die Login-Daten (PIN) und Geldtransferautorisierungsdaten (TAN) nur auf der überprüften Internet-Banking-Seite des Geldinstituts ein, zu dem eine Kontoverbindung besteht. Niemals dürfen diese vertraulichen Daten in E-Mails, Formularen oder unbekannten Internet-Banking Systemen eingegeben werden."

5. Internet-Banking-Adresse (URL) nur manuell eingeben: „Folgen Sie niemals Links aus E-Mails oder von anderen Internet-Seiten zum (vermeintlichen) Internet-Banking-Portal der Hausbank. Auch die Verwendung von Bookmarks birgt Gefahrenpotenzial, da sie von Hackern manipuliert werden können. Deaktivieren Sie die Auto-Vervollständigungsfunktion im Browser, um nicht versehentlich auf eine falsche Web-Seite zu gelangen."

6. Internet-Banking-Seiten prüfen: „Die Webseite Ihrer Bank sollten Sie genau lesen und aufschreiben, damit Sie sie beim nächsten Einloggen sofort wieder erkennen. Achten Sie auf eine sichere, verschlüsselte Verbindung. Diese erkennen Sie daran, dass in der Adressleiste des Browsers ‚https://...' angezeigt wird. Prüfen Sie auch, ob die Verschlüsselung mittels digitalem Sicherheitszertifikat aktiviert ist. Dazu genügt ein Klick auf das Schloss-Symbol im Browser rechts unten. Wird in der Adressleiste hingegen lediglich ‚http://...' angezeigt, erfolgt die Übertragung von Daten unverschlüsselt und ist daher zu unsicher für Online-Bankgeschäfte.

7. Benutzer-PIN und TAN nicht am Computer ablegen: „Verwahren Sie Ihre vertraulichen Bankinformationen an einem sicheren Ort. PCs sind dafür nicht geeignet. Sollten Sie PIN und TAN dennoch auf Ihrem Computersystem speichern wollen, dann nur verschlüsselt und niemals im Browser selbst!"

8. Vorsicht bei angeblichen Banken E-Mails: „Österreichische Bankinstitute versenden grundsätzlich keine E-Mails, in denen Kunden aufgefordert werden, vertrauliche Zugangs- und Transaktionsinformationen preiszugeben. Dazu zählen Verfügernummer, PIN und TAN. Bei dieser Art von E-Mails handelt es sich immer um Betrugsversuche."

9. Bankeninfos beachten und Vorfälle der Bank-Hotline melden: „Beachten Sie die Sicherheitshinweise Ihrer Hausbank auf der entsprechenden Internet-Homepage. Sobald der Verdacht auf Betrug entsteht, geben Sie keinerlei Daten Preis und melden Sie Ihren Verdacht der jeweiligen Bank-Hotline. Bei sicherheitsrelevanten Vorfällen sollte der PIN schnellstmöglich über eine sichere Verbindung geändert werden."

10. Kontoauszüge regelmäßig prüfen: „Überprüfen Sie in regelmäßigen Abständen Ihre Kontoauszüge auf Unregelmäßigkeiten. Achten Sie auch besonders auf E-Mails in denen angebliche Finanzagenten Ihnen einen Gewinn z. B. bei der Euro Millionen Lotterie ankündigen und Sie bitten, einen Betrag zu beheben und rasch an ein anderes Konto zu überweisen. Achtung: Sie werden hier zur Geldwäsche missbraucht und machen sich strafbar!"

Ursprung: http://krone.at/ 02/2007