



Gemeinsames Präventionsprojekt von Polizei und VKP **Gefahr durch neue Medien – Wie sicher Sie leben, entscheiden Sie selbst!**

Serienbeitrag 2: Sicheres Homebanking

Sicherlich ist es bequem, seine Bankgeschäfte von zu Hause abzuwickeln, trotzdem gilt auch hier :

„Ohne ein Mindestmaß an Medien-Kompetenz und Computer-Sicherheit sollte man unbedingt Abstand vom Online-Banking nehmen !“

Vor dem Hintergrund einer stetig steigenden Service-Nachfrage treffen die Kreditinstitute zwar umfangreiche Sicherungsmaßnahmen, um Ihre Internet-Kunden zu schützen. Diesen Schutz versuchen Kriminelle jedoch auszuhebeln und nutzen dabei die Leichtgläubigkeit ihrer Opfer.

Ihre Masche: Sie versenden fingierte E-Mails, so genannte Phishing-Mails. Diese sollen den Empfänger dazu veranlassen, persönliche Daten wie Zugangsdaten, Passwörter, Transaktionsnummer usw. Preis zugeben.

Dabei werden die Methoden immer raffinierter. Kamen früher Mails im Umlauf, die - einfach gestrickt und schlecht formuliert - die Absicht des Absenders auf Anheb verrieten, so ködern die Täter ihre Opfer heute mit professionell gestalteten Internet-Seiten, die selbst von Profis nur schwer als "Fälschung" zu identifizieren sind.

Bewahren Sie sich gegenüber elektronischer Post ein **gesundes Misstrauen** – selbst dann, wenn die Homepages mit bekannten Symbolen und in vertrauter Gestaltung aufwarten.

- Tragen Sie die Internet-Adresse Ihrer Hausbank in die **Favoritenliste** Ihres Browsers ein und benutzen Sie diese ! Folgen Sie weder in E-Mails angegebenen Links oder den Ergebnissen eines Such-Anbieters wie Google pp., um zur Homepage Ihrer Hausbank zu gelangen !
- Geben Sie weder PIN noch TAN in plötzlich auftauchenden **PopUp**-Fenstern ein !
- Seriöse Banken und Kreditinstitute fordern **niemals** vertrauliche Daten per E-Mail oder per Telefon von Ihnen an. In solchen Fällen halten Sie sofort persönliche Rücksprache mit Ihrem Kundenberater der Hausbank.

- Sollte Ihnen etwas merkwürdig vorkommen, **beenden** Sie die Verbindung und **stoppen** Sie die Transaktion. Selbst kleinste Veränderungen sollten Sie misstrauisch machen !!
- Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich **korrekt abmelden**. Es reicht nicht, das Browserfenster über das Funktionskreuz (oben rechts) zu schließen.
- Während des Homebankings sollten Sie alle anderen **Anwendungen** schließen ! Surfen Sie also nicht gleichzeitig auf verschiedenen Seiten.
- **Kontrollieren** Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen. So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben.
- **PIN** und **TAN** sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist : Die Adresszeile beginnt mit **https://** ...
Im Browserfenster erscheint ein kleines Symbol, z.B. in Form eines Vorhängeschlosses, das den jeweiligen Sicherheitsstatus symbolisiert.
- Falls Sie externe **Zugangs-Software** nutzen, so stellen Sie sicher, dass es sich dabei um die offizielle und aktuelle Version Ihrer Bank handelt.
- Benutzen Sie für Ihren Computer immer **komplexe Passwörter**, die Sie regelmäßig ändern !
- **Vernichten** Sie nicht mehr benötigte Dokumente, beispielsweise die Zugangsdaten Ihrer Bank oder bewahren Sie diese an einem sicheren, nicht zugänglichen Ort auf.
- Ein hohes Maß an Sicherheit bieten Homebanking-Programme, die eine Offline-Eingabe ermöglichen. Noch besser: Sie entscheiden sich für die Teilnahme am Home-Banking mit Chipkarte und Kartenlesegerät, welches sie u.U. bei Ihrer Hausbank anfordern können.
- Halten Sie Ihren Rechner auf dem neuesten Stand. Nutzen Sie die automatische **Update**-Funktion des Herstellers Ihres Betriebssystems und wählen Sie die höchstmögliche Sicherheitseinstellung in Ihrem Computer.
- **Verwenden** Sie auf Ihrem Computer stets und ausnahmslos Anti-Virus-Software, sog. Viren-Scanner und zusätzlich die sog. Personal Firewall.
- **Besonders wichtig** : Führen Sie Bankgeschäfte nur an Rechnern durch, denen Sie wirklich vertrauen können. Es gibt nämlich Programme oder technische Einrichtungen, die Ihre Eingaben mitloggen können, ohne dass Sie es merken.
--> **Verzichten** Sie deshalb unbedingt darauf, Ihre Bankgeschäfte in Internet-Cafes, am Hotel-Computer oder im Urlaub / Ausland zu erledigen, sondern erledigen Sie dies ausschließlich von zu Hause !

Für einen größtmöglichen Schutz können Sie selber sorgen :

- **Verzichten** Sie auf ein wenig Komfort und bemühen Sie sich persönlich zu Ihrer Hausbank !
- Und wenn Sie Ihre Überweisungen weiterhin schriftlich tätigen wollen, werfen Sie diese nicht am Briefkasten ein, sondern übergeben Sie sie einem / einer Mitarbeiterin der Bank **persönlich während der Öffnungszeiten.**

Weitere Informationen finden sie unter:

www.bsi-fuer-buerger.de

Die Beauftragte für Kriminalprävention der Polizei, Polizeioberkommissarin Katja Reents, bietet darüber hinaus Vorträge und persönliche Beratungen zu diesem Thema an. Sie ist dienstlich unter der Rufnummer 04421-942-108 zu erreichen.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung:

Markus Wallenhorst
Presse- und Öffentlichkeitsarbeit
Polizeiinspektion
Wilhelmshaven/Friesland
04421-942-404
markus.wallenhorst@polizei.niedersachsen.de

Andrea Papenroth,
Pressesprecherin des VKP,
Tel. 04421-942-437
andrea.papenroth@polizei.niedersachsen.de