



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

### **Serienbeitrag Nr. 7 - Phishing - Attacken**

" Phishing " ist prinzipiell nichts anderes als eine Vorbereitungshandlung für klassischen Betrug und Diebstahl, weil das Vertrauen und die Arglosigkeit von Menschen ausgenutzt werden, um Sie später zu betrügen und zu bestehlen ! Ihnen wird praktisch vorgegaukelt, Sie würden sich auf der echten Internet-Präsenz Ihrer Hausbank bewegen. In Wirklichkeit werden Ihre geheimen Konto-Zugangsdaten gestohlen und später missbraucht.

### **Phishing = Passwort fischen ( geheime Daten ausspionieren )**

Häufigste Verbreitungsmethode : Per eMail verschickte Fragebögen, die den Anschein erwecken sollen, als stammen diese von Ihrer Hausbank.

In letzter Zeit nehmen auch sogenannte PopUp-Fenster zu, die Sie zu einer Homepage weiterleiten, die der Internetpräsenz Ihrer Hausbank täuschend ähnlich sieht. Wenn Sie darauf hereinfallen und das dort hinterlegte Angebot nutzen, ist der finanzielle Schaden praktisch schon entstanden !

Ärger haben auch die Unternehmen, in deren Namen die Betrüger auftreten. Denn sie erleiden oft einen Image-Schaden. Prominente Beispiele hierfür sind eBay, die Deutsche Telekom AG oder die Deutsche Bank.

Haben Sie persönlich den Verdacht, Opfer einer Phishing-Attacke geworden zu sein, heißt es **schnell zu handeln** :

- **Sperren** Sie sofort den Zugang für das betroffene Konto bei Ihrer Hausbank ! Entweder direkt oder über die bundesweite Telefon-Hotline :

**116 116 !**

- **Prüfen** Sie über einen Kontoauszugsdrucker ( nicht über den infizierten Computer ! ), ob unrechtmäßige Konto-Verfügungen vorgenommen wurden.
- **Drucken** Sie betrügerische Mails, die Sie erhalten haben, einschließlich der vollständigen Kopfzeile, dem sog. „ Header “ aus.
- **Erstatten** Sie im Schadensfall Anzeige bei der Polizei !

- **Kontrollieren** Sie Ihren Computer auf eine mögliche Infizierung, z.B. durch den Symantec Security Check, einem kostenlosen Angebot des Sponsors Symantec !
- **Unterbrechen** Sie den Zugang zum Internet ( Router abschalten) und bereinigen Sie den PC mithilfe professioneller Sicherheitslösungen, bis Sie sicher sein können, dass das sog. Schad-Programm beseitigt wurde.
- **Ändern** Sie Ihre Passwörter sämtlicher Anwendungen !

Außerdem gilt der grundsätzliche Tipp von Polizei und VKP-WHV :

**Wenn Sie der Meinung sind, dass Sie Ihren Computer nicht wirksam vor den Risiken des Internets schützen können, sollten Sie wenigstens auf Online-Banking verzichten !**

Ihr Geschäftspartner kann lieber einen Tag länger auf sein Geld warten, als dass Sie hinter Ihrem gestohlenen Geld hinterher laufen müssen. Denn eine Schadensregulierung durch die Hausbank hängt oftmals nur von der Kulanz des Unternehmens ab. Sie haben möglicherweise keinen Anspruch auf Schadenersatz, insbesondere nicht, wenn Sie grob fahrlässig gehandelt haben.

Klassisches Beispiel :

Häufig steht in Phishing-Mails so gut wie nie der eigene Name, unpersönliche Formulierungen wie " Sehr geehrter Kunde " oder " Lieber Mitarbeiter " sind die Regel. Meist wird in den ersten Sätzen gleich versucht, den Adressaten zu überrumpeln. Sätze wie " Wenn Sie nicht innerhalb der nächsten zwei Tage eine Verifikation durchführen, wird ihr Konto / ihre Kreditkarte gesperrt " sind typisch für Phishing-Mails.

Deshalb gilt :

- Seien Sie stets misstrauisch und nehmen Sie sich Zeit, Internetseiten zu prüfen, bevor Sie in etwaige Fallen tappen und dort hinterlegte Angebote nutzen !
- Klicken Sie nicht unbedacht auf plötzlich auftauchende Bilder oder Mitteilungen !
- Kein seriöses Unternehmen - weder Ihre Hausbank noch Ebay oder sonstige akkreditierte Unternehmen - wird Sie jemals per Mail auffordern, zu einer bestimmten Internetseite zu gehen und dort Ihre persönlichen Daten einzugeben oder zu aktualisieren.

**So können Sie die Gefahren reduzieren :**

- **Textformat in Mails:** Die meisten Mailprogramme bieten Ihnen die Auswahl, ob Sie Mails im html-Format erhalten möchten oder im reinen Textformat. **Entscheiden Sie sich für das Textformat.** Die eMails mögen dann nicht mehr so farbig sein; irreführende Links - und andere Gefahren - gehören dann aber der Vergangenheit an.
- **Seitenbesuch:** Besuchen Sie Webseite Ihrer Hausbank immer über das Lesezeichen in Ihrem Browser oder geben Sie die Adresse manuell in die Adressleiste des Browsers ein. Folgen Sie niemals dubiosen „ Links “, die Ihnen in dubiosen Mails angezeigt werden oder als Ergebnis einer Suchmaschine wie Google angezeigt werden.

- **Information:** Wenn Sie eine verdächtige Mail - gleich welcher Art - erhalten, überprüfen Sie in den gängigen Suchmaschinen, was es damit auf sich hat. Geben Sie hierbei passende Stichworte ein, etwa den Namen des vermeintlichen Absenders und den Begriff "Mail", "Phishing", oder auch "Betrug".
- **Technischer Schutz:** Ein aktuelles Antiviren-Programm und eine FireWall gehören auf jeden PC. Aber **Achtung** : Dieser Schutz funktioniert nicht so perfekt, wie Sie es gerne hätten ! Zwar sind die Schutzprogramme ein wichtiger Baustein für den Phishing-Schutz und unverzichtbar, aber den eigentlichen Anwendungsfehler macht niemals der Computer, sondern Sie ! Verlassen Sie sich also nicht zu sehr auf Ihre Sicherheits-Software und seien Sie stets skeptisch !

---

Siehe dazu auch : [www.bsi-fuer-buerger.de](http://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](mailto:markus.wallenhorst@polizei.niedersachsen.de)

Andrea Papenroth, Pressesprecherin des  
VKP,  
Tel. 04421-942-437  
[andrea.papenroth@polizei.niedersachsen.de](mailto:andrea.papenroth@polizei.niedersachsen.de)