

## GEMEINSAM.SICHER gegen Phishing

Phishing ist ein Versuch persönliche Daten über das Internet zu erlangen. Über E-Mails und betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kennwörter, Kontodaten usw. abzufragen. Phishing gibt es in unterschiedlichsten Varianten. Fingierte E-Mails etwa sollen beim Nutzer den Eindruck erwecken, sie kämen von seiner Bank oder einem Online-Auktionshaus. Die Empfängerin oder der Empfänger wird aufgefordert, einen Link anzuklicken - vom dem er zu einer meist täuschend echt aussehenden Betrugs-Webseite geleitet wird. Dort wird der Nutzer unter einem Vorwand gebeten, seine persönlichen Daten – darunter auch Passwörter – einzutragen.

**Bei Verdachtsmomenten kontaktieren Sie bitte sofort Ihr Bankinstitut!**

### Tipps Ihrer Polizei:

- Kein seriöses Unternehmen oder Bankinstitut fordert per E-Mail zur Eingabe von persönlichen Daten wie Passwörter usw. auf.
- Internetseiten, auf denen man sensible Nutzerdaten eingeben muss, erkennen Sie an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Weiters sind sichere Webseiten auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat.
- Überprüfen Sie die Adresszeile des Webbrowsers. Oft reicht ein Blick, um zu erkennen, dass es sich gar nicht um die richtige Website handelt.
- Richten Sie sich Ihre wichtigen Homepages wie zum Beispiel Bankzugang etc. als Favoriten in Ihrem Browser ein und verwenden Sie nur diese. So stellen Sie sicher, dass Sie nur die offiziellen Seiten verwenden.
- Wichtig ist der Schutz durch Passwörter: Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste. Je länger ein Passwort, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und Sonderzeichen verwendet (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren.“ ergäbe das Passwort: Iba1.J1970g.)
- Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken.
- Sind Sie sich unsicher, ob Sie ein Passwort bekannt gegeben haben, dann ändern Sie als erstes das Passwort und melden Sie diesen Vorgang an die Betreiber der Homepage bzw. des Unternehmens.

**Einen schönen und sicheren Sommer wünscht Ihnen**

**Ihr GEMEINSAM.SICHER – Team**

**133 Ihre Polizei – immer für Sie da!**