

Checkliste **Verhaltensregeln zum Vorbeugen von Phishing-Schäden**

- Wählen Sie für Ihre Online-Dienste sichere und unterschiedliche Passwörter.
- Seien Sie immer misstrauisch, wenn jemand vertrauliche Informationen von Ihnen erbittet.
- Wenn Sie angeblich E-Mails von Ihrer Bank oder einem anderen Online-Dienstanbieter (Paypal, ebay, etc.) erhalten, überlegen Sie, ob der vermeintliche Absender überhaupt Ihre E-Mail-Adresse kennen kann.
- Wollen Sie einen bestimmten Online-Dienst nutzen, dann geben Sie die entsprechende Internetadresse von Hand ein. Bei Ihrem Besuch der angeforderten Website können Sie die von Ihnen eingegebene Adresse als Favorit beziehungsweise Lesezeichen (Bookmark) in Ihrem Browser abspeichern.
- Verdächtige E-Mails sollten Sie sofort löschen ohne sie öffnen.
- Öffnen Sie in E-Mails von Unbekannten keine darin enthaltenen Links und keine darin enthaltenen E-Mail-Anhänge.
- Reagieren Sie nicht auf Instant-Messenger-Nachrichten, SMS oder MMS von Unbekannten.
- Geben Sie keine vertraulichen Informationen an unbekannte (Internet-)Telefonanrufer weiter.
- Geben Sie nie vertrauliche Informationen auf unbekanntem Webseiten preis.
- Geben Sie prinzipiell nie vertrauliche Informationen preis, wenn Sie sich nicht absolut sicher sind, wo diese landen werden.
- Überprüfen Sie stets die Aktivitäten Ihrer Online-Konten, zum Beispiel beim Online-Banking den Kontoauszug oder bei Online-Auktionshäusern Ihre Ein- und Verkäufe.
- Setzen Sie für Ihr Konto ein Überweisungslimit fest.
- Gehen Sie umsichtig mit Ihren Passwörtern, PINs sowie TANs um. Beachten Sie hierzu unsere Checklisten **Sicherer Umgang mit der PIN** und

Sicherer Umgang mit TANs.

- Wenn Sie eine Phishing-E-Mail entlarvt haben, nehmen Sie bitte Kontakt zum betroffenen Dienstleister auf, damit er andere Kunden zum Beispiel durch eine Warnung schützen kann.
- Benutzen Sie keine fremden oder öffentliche Computer, wie zum Beispiel in einem Internetcafé, um Online-Geldgeschäfte zu tätigen.