WEISSER RING
Wir helfen Kriminalitätsopfern.

Konkrete Präventionstipps zum Thema Phishing

- Nutzen Sie den „gesunden Menschenverstand“: Bei unbekanntem Absender, Rechtschreibfehlern, unbekannter Aufforderung zur Zahlung oder Mahnung, E-Mail-Anhang ohne Inhalt, unbekanntem Link oder unbekannter Weiterleitung – auf solche Nachrichten nicht antworten und keine Dateianhänge oder Links öffnen!
- Auch bei unangekündigten Dateianhängen von bekannten Absendern nicht gleich öffnen, sondern gegebenenfalls beim Mailkontakt nachhaken, ob der Anhang vom Versender stammt. Lieber einmal zu viel gefragt, als einmal zu wenig.
- Achten Sie auf eine sichere Verbindung zum Browser: Neben dem https:// ist auch das Schlosssymbol in der Adressleiste ein Hinweis auf eine sichere Verbindung. Ist es geschlossen ist die Internetverbindung gesichert, ist es hingegen geöffnet, besteht keine sichere Verbindung.
- Vertraulichen Daten (PINs, TANs, Passwörter usw.) werden von seriösen Banken grundsätzlich nicht per E-Mail, Telefon oder Post bei Ihnen abgefragt. Im Zweifel kontaktieren Sie Ihre Bank.
- Veränderungen im Ablauf des Online-Bankings sollten Sie misstrauisch machen. Geben Sie persönliche Daten nur bei gewohntem Verlauf innerhalb des Online-Banking an. Sollte Ihnen etwas seltsam vorkommen, beenden Sie die Verbindung und versuchen Sie es erneut.
- Melden Sie sich beim Beenden Ihrer Onlinebanking-Geschäfte ab. Schließen Sie nicht bloß das Browserfenster. Wechseln Sie vor Ihrer Abmeldung nicht auf eine andere Internet-Seite.
- Kontrollieren Sie Ihr Konto. Sollten Sie hierbei Auffälligkeiten feststellen, können Sie schnell reagieren, ihre Bank informieren und das Konto gegebenenfalls sperren lassen.