

Checkliste: Technische Hilfsmaßnahmen gegen Phishing

Sicher eingerichteter Computer

- Konnten Sie alle Punkte unserer Checkliste **Sicherer Computer** abhaken?

Abgesicherter Netzwerkzugang

- Benutzen Sie einen vertrauten, nicht öffentlichen Internetzugang.
- Benutzen Sie kein ungeschütztes, unbekanntes WLAN.

Phishing-vorbeugende Einstellung Ihres E-Mail-Programms

- Deaktivieren Sie in Ihrem E-Mail-Programm die HTML-Darstellung. Dies verringert die Gefahr, dass sich Schadsoftware auf Ihrem Computer installieren kann oder Linkziele mit Hilfe zusätzlicher Formatierungen verschleiert werden können.
- Deaktivieren Sie in Ihrem E-Mail-Programm die automatische Vorschaufunktion für E-Mail-Anhänge. Dies verringert die Gefahr, dass sich Schadsoftware auf Ihrem Computer installieren kann.
- Verschicken Sie selbst E-Mails möglichst nur im Textformat.

Phishing-vorbeugende Einstellung Ihres Browser

- Deaktivieren Sie das automatische Ausführen von Skripten beziehungsweise aktiven Inhalten.
- Speichern Sie Ihre Online-Dienste als Favorit beziehungsweise als Lesezeichen (Bookmark) ab und nutzen Sie diese wenn Sie die entsprechenden Seiten besuchen wollen.

Zusätzlich technische Hilfsmittel zur Erkennung von Phishing-Attacken

- Installieren Sie zusätzliche Browser-Erweiterungen, die Sie vor bekannten Phishing Seiten warnen, zum Beispiel die Netcraft-Toolbar für den Internet Explorer sowie Firefox-Webbrowser.
- Installieren Sie eine Anti-Spam-Lösung für spezielle E-Mail-Programme, zum Beispiel SPAMfighter für Outlook/Express, Windows Mail und Thunderbird. Hintergrund: Viele Spam-E-Mails sind Phishing-Versuche.

- Installieren Sie eine Sicherheitskomplettlösung mit Anti-Phishing-Option, zum Beispiel Avira Antivir für Windows sowie Linux.