

Zunächst einmal: Sicherheit am PC

Ohne einen ausreichend geschützten PC erzielen Sie auch keine 100%ige Sicherheit im Online-Banking und beim Online-Shopping.

Nutzen Sie im Falle der Fälle die „Digitale Rettungskette“!

1. Virenschutzprogramm und Firewall installieren und aktuell halten.
2. An öffentlichen PCs keine vertraulichen Daten eingeben.
3. Nicht als Administrator am PC arbeiten.
4. Keine Zugangsdaten im Browser oder auf der Festplatte speichern.
5. Sicherheitsupdates des Betriebssystems/der Software durchführen (Empfehlung: Programme wie z.B. UpdateStar).
6. Komplexe Passwörter verwenden & regelmäßig ändern (Empfehlung: 1 Mal pro Monat und bei jedem Dienst ein anderes Passwort verwenden!) – Achtung vor Phishing & Spam! Prüfung über [Pwned-Webseite](#) oder [Identity Leak Checker](#) des HPI!
7. Auf Sicherheit der Seite achten: „https“!
8. Vorsicht beim Öffnen von Anhängen von E-Mails (insbesondere ausführbare Dateien, z.B. EXE, aber auch Bilder)
9. Bei VoIP und WLAN verschlüsselte Kommunikation (WPA/WPA2).
10. Zurückhaltung im Social Media (XING, Facebook, Twitter, etc.) mit persönlichen Informationen.
11. Regelmäßige Backups von Daten.