

## Checkliste Was tun, wenn Sie vermuten, Phishing-Opfer geworden zu sein?

---

Wenn Sie Opfer eines Phishing-Angriffs geworden sind, kommt es auf schnelles und richtiges Handeln an, um den Schaden zu minimieren.

### Reaktion auf verdächtige Ereignisse, wie beispielsweise Fehlermeldungen

- Melden Sie sich von dem betroffenen Konto umgehend ab (ausloggen).
- Überprüfen Sie, ob Ihr Anti-Viren-Programm auf dem aktuellsten Stand ist und überprüfen Sie Ihren Computer auf Schadsoftware. Überprüfen Sie das Protokoll des Suchverlaufs Ihres Anti-Viren-Programms. Wenn Sie Schadsoftware finden, melden Sie sich auch bei anderen Online-Diensten ab. Speichern Sie das Protokoll ab und drucken Sie es zusätzlich aus.
- Melden Sie sich mit einem anderen Browser wieder an und kontrollieren Sie Ihre zuletzt durchgeführten Aktionen. Benutzen Sie dazu möglichst ein anderes Benutzerkonto oder am besten einen anderen Computer.

### Entdeckte Unregelmäßigkeiten oder tatsächliche Schäden

- Kontaktieren Sie umgehend Ihren Dienstanbieter (Bank oder Versandhaus, etc.), wenn Sie Unregelmäßigkeiten, wie zum Beispiel eine von Ihnen nicht getätigte Überweisung, finden.
- Sollte Schaden entstanden sein, wenden Sie sich sofort an die **Polizei**. Nehmen Sie keine Änderungen mehr an Ihrem Computer vor.

### Zugang zum Online-Dienst

- Ändern Sie sofort Ihre Zugangsdaten des betroffenen Dienstes am besten mit einem anderen abgesicherten Computer.
- Sollten Sie sich nicht mehr Anmelden können, um Ihre Zugangsdaten zu ändern, geben Sie möglichst oft ein falsches Passwort ein. Beim Online-Banking bewirkt dies eine Sperrung des Online-Banking-Kontos, so dass der Phisher auch keinen Zugang mehr hat.

### Mitbenutzer warnen

- Warnen Sie alle Mitbenutzer des Computers.