# Der beste Schutz für Ihr Geld: Sie.

## Gemeinsam gegen Online-Trickbetrug.

**Modernes und sicheres Online-Banking:** Dafür steht Ihre Sparkasse. Weit über die gesetzlichen Anforderungen hinaus nutzen wir vielfältige Möglichkeiten, um Betrug und Manipulation zu verhindern.

**Doch wir brauchen Sie,** Ihre Aufmerksamkeit und Ihr gesundes Misstrauen. Denn wenn Sie selbst etwa Geld an unseriöse Empfänger überweisen oder Schadsoftware herunterladen: Dann hilft oft auch der beste Schutz nicht.

## Die gängigen Varianten: Telefon, Fernzugriff oder große Versprechen

So manches Opfer hätte nie gedacht, dass es auf eine dieser Maschen hereinfällt. Deshalb ist es wichtig, sie zu kennen und zu erkennen:

1. **Anruf:** Angebliche Mitarbeitende Ihrer Sparkasse oder von Behörden (Polizei, Staatsanwaltschaft etc.) rufen Sie an, möglicherweise sogar mit manipulierter Rufnummernanzeige. Über gestohlene Passwörter konnten persönliche Daten der Opfer ermittelt werden, mit deren Hilfe versucht wird, das Vertrauen zu erschleichen. Zeit- oder psychologischer Druck (mit oft vorgetäuschten familiären Katastrophen) sollen Sie dazu bringen, Geld zu überweisen, eine Freigabe vorzunehmen, Zugangsdaten zu verraten oder Schadsoftware zu installieren. Oft wird gar behauptet, dass damit ein Betrug gestoppt oder aufgedeckt werden soll.

**Folgen Sie den Anweisungen keinesfalls und beenden Sie das Gespräch!** Sparkassen- oder Behörden-Mitarbeitende würden so etwas nie tun.

2. **Fernzugriff:** Per Telefon, Mail oder versehentlich installierter Schadsoftware werden Sie aufgefordert, Zugriff auf Ihren PC oder Ihr Smartphone zu gewähren. Oft sind es angeblich Microsoft- oder HelpDesk-Mitarbeitende. Sie geben vor, ein technisches Problem lösen oder ein Update vornehmen zu wollen. Auch hier werden Sie unter Druck gesetzt, sollen Vorgänge durch Ihre Freigabe autorisieren, Daten und/oder Passwörter eingeben etc.

**Lassen Sie niemals Unbekannte auf Ihren PC oder Ihr Smartphone zugreifen!** Denn so verlieren Sie die Kontrolle. Oft bekommen Sie nicht einmal mit, was im Hintergrund passiert. Legen Sie sofort auf, installieren Sie keine unbekannten Programme, kontrollieren Sie alle Transaktionsdaten, bevor Sie diese freigeben.

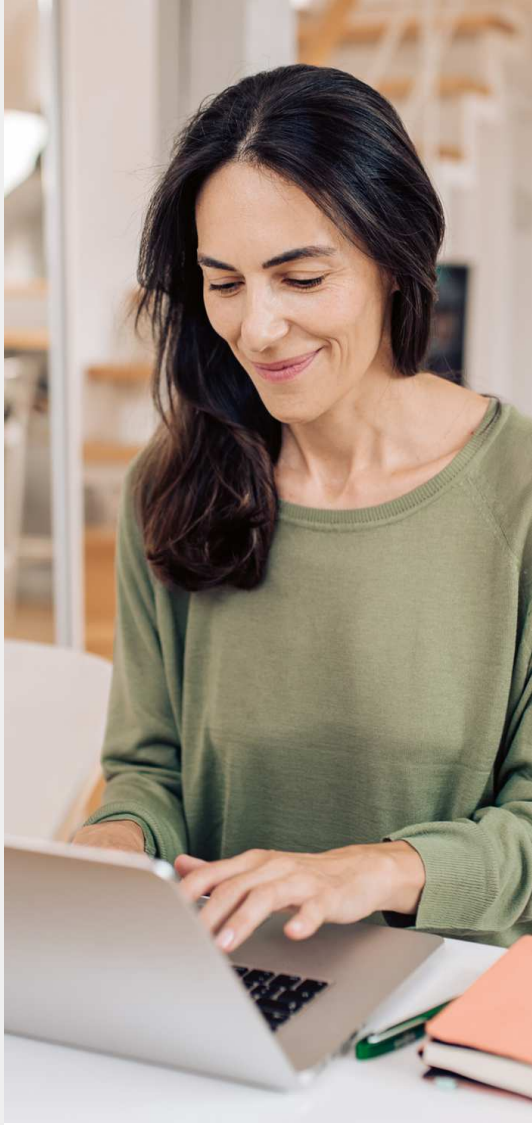
3. **Lukrative Geldanlagen** sollen Sie locken, Ihr Geld in unseriöse oder gänzlich gefälschte Finanzanlagen oder dubiose Kryptowerte zu stecken – und zu verlieren. Oft ähneln die Fake-Anbieter nahezu exakt echten, seriösen Unternehmen, z. B. mit identisch aussehenden Internetseiten.

**Seien Sie bei Geldanlagen im Internet generell äußerst vorsichtig!** Recherchieren Sie stets gründlich: Ist die erwartete Rendite überhaupt realistisch? Wird Druck aufgebaut? Ist das Impressum echt und wo sitzt das Unternehmen? Wohin soll das Geld überwiesen werden?

## Sie haben einen Verdacht?

Folgen Sie keinen verdächtigen Anweisungen. Nehmen Sie Kontakt zu uns auf – oder in dringenden Fällen direkt mit der Polizei.
Weitere Informationen zu Betrugsmaschen sowie Sicherheitshinweise finden Sie unter: www.berliner-sparkasse.de/sicher





Berliner Sparkasse
Alexanderplatz 2
10178 Berlin
Telefon: 030/869 86969
info@berliner-sparkasse.de

**Weil's um mehr als Geld geht.**