6 aktuelle Betrugsmaschen im Überblick

Masche	Ziel der Täter	So schützen Sie sich	Maßnahmen für Opfer
Darcula-Phishing	Gefälschte SMS von Paketdiensten; Datendiebstahl über realistisch wirkende Webseiten.	Keine Links aus Nachrichten anklicken; Browser mit Phishing-Blocker nutzen; Sicher mit Kreditkarte bezahlen, am besten mit Käuferschutz.	Karte sperren, Bank informieren, Anzeige erstatten.
PhaaS (Phishing-as-a-Service)	Kriminelle mieten Baukästen für Phishing-Kampagnen.	E-Mails kritisch prüfen; Sicherheitssoftware nutzen; niemals sensible Daten preisgeben.	Passwörter ändern, Banken benachrichtigen, Konten überwachen.
Quishing (QR-Code-Phishing)	QR-Codes in Mails oder Briefen führen auf gefälschte Seiten.	Nur QR-Codes von seriösen Quellen scannen; Adresse nach Scan prüfen. Daten eingegeben?	Sofort Bank informieren und Kennwörter ändern.
Vishing	Telefonbetrug durch vermeintliche Bankmitarbeiter.	Keine Daten am Telefon preisgeben; bei Unsicherheit Rückruf bei offizieller Banknummer.	Gespräch beenden; Bank informieren; Anzeige erstatten.
Deepfake-Betrug	Sprach- oder Video-Deepfakes, die Vertrauen erschleichen.	Identität verifizieren (z. B. durch Rückruf oder Videocall mit Sicherheitsfrage).	Anzeige erstatten; Daten absichern; Bank informieren.
Gefälschte Finanzplattformen	Täuschend echte Investitionsportale locken mit Versprechen hoher Rendite.	Anbieter über BaFin prüfen; bei unrealistischen Angeboten skeptisch bleiben.	Nicht nachinvestieren; rechtlichen Beistand suchen; Anzeige erstatten.

Stand: Mai 2025

Kostenlose-Kreditkarte .de