Juni 2025

VR Aktuell

EIN THEMA. VIELE FACETTEN.

Gut geschützt gegen Betrug

1 *VORSICHT FALLE*
Phishing und Fake-Shops erkennen

2 *TELEFON-SCHWINDEL*
Manipulation und Täuschung stoppen

3 *SELBSTSCHUTZ PER SMS-REGEL*
Sicher bleiben mit drei Schritten

Gängige Maschen und wie Sie sich absichern

Digitale Welt im Alltag

Wir leben in einer zunehmend digitalisierten Welt. Kundinnen und Kunden in Deutschland erwarten heute selbstverständlich jederzeit verfügbare Online-Angebote und schnelle, digitale Zahlungsverfahren. Große Online-Plattformen, aber auch immer mehr mittelständische und kleine Händler bieten ihre Waren und Dienstleistungen rund um die Uhr an. Für sichere Zahlungen – sowohl beim Einkauf vor Ort als auch im E-Commerce – sorgen Banken und andere Zahlungsdienstleister mit leistungsfähigen, verlässlichen Lösungen.

Betrug erkennen und vermeiden

Doch auch die beste Technik bietet keinen absoluten Schutz, wenn man unvorsichtig damit umgeht. Betrüger entwickeln ständig neue Methoden, um Schwachstellen und Unachtsamkeit im Umgang mit digitalen Angeboten auszunutzen. In dieser Ausgabe von VR Aktuell erfahren Sie, wie Sie die häufigsten Betrugsmaschen wie Phishing, Fake-Shops, Social Engineering und falsche Anrufe erkennen und vermeiden können. Sie erhalten klare Informationen zu den Tricks der Betrüger sowie drei einfache Verhaltensregeln, die Ihre Sicherheit im Internet entscheidend erhöhen.

1 VORSICHT FALLE
PHISHING UND FAKE-SHOPS ERKENNEN

Phishing

Besonders häufig spähen Kriminelle die Internetnutzenden mit Phishing-Mails oder Schadsoftware aus. Beim Phishing versuchen Internetbetrügende, durch gefälschte E-Mails, Briefe oder SMS an PIN, Passwörter oder TAN zu kommen. Hierzu versenden die Täter fingierte Phishing-Nachrichten oder treten in sozialen Netzwerken als vertrauenswürdige Personen auf, um den Nutzern ihre Daten abzuluchsen. Fast jede dritte unerwünschte E-Mail mit Werbung, vermeintlichen Gewinnbenachrichtigungen oder unbestellten Newslettern ist laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Phishing-Versuch. Über 62 Prozent der Nutzenden haben schon mal wissentlich eine Phishing-E-Mail erhalten.

Phishing-E-Mails enthalten in der Regel Links oder Schaltflächen, die Links verstecken. Diese führen auf professionell gestaltete Webseiten, auf denen die Opfer ihre persönlichen Zugangsdaten, Passwörter und TANs eingeben sollen. Typisch für Phishing-Mails: Die Opfer werden stark unter Druck gesetzt mit der Behauptung, dass bei Nichthandeln ihr Bankkonto oder ihr Shopping-Zugang gesperrt oder gelöscht wird und Transaktionen dann nicht mehr möglich sind. Noch Schlimmeres kann passieren, wenn man über solche Links Programme lädt und startet, die den Rechner oder das Smartphone dauerhaft infizieren. Phishing gibt es genauso auch per Brief mit offiziell aussehenden Logos bekannter Banken oder Unternehmen. Diese enthalten dann QR-Codes, die Nutzende scannen sollen, um auf Phishing-Seiten zu kommen. Mit den abgefischten persönlichen Daten können die Betrügenden persönliche Informationen erlangen, im Namen des Opfers Online-Käufe durchführen oder falsche Informationen verbreiten.

Bitte beachten!

- Geben Sie die persönlichen Zugangsdaten nur auf der bekannten Webseite der Bank, des Zahlungsdienstleisters oder des Online-Handels ein.
- Klicken Sie niemals auf Links in unerwarteten E-Mails oder SMS, sondern löschen Sie diese sofort.
- Kreditinstitute oder Online-Dienste werden niemals E-Mails oder Schreiben versenden, die zur Eingabe persönlicher Zugangsdaten auf fremden Webseiten auffordern.
- Bestehen hier Zweifel, ist es empfehlenswert, sich zu der jeweiligen Nachricht bei der Bank oder dem potenziellen Anbieter direkt zu erkundigen.

Fake-Shops

99 Prozent der Internetnutzenden in Deutschland kaufen laut einer Umfrage des Branchenverbands Bitkom online am PC oder über ihr Smartphone ein, acht Prozent sogar täglich. Doch nicht alle Geschäfte im Netz sind sicher. Internetkriminelle locken Verbraucher mit betrügerischen Produkten oder Dienstleistungen auf Plattformen oder in sogenannten Fake-Shops. Fake-Shops sind oft Kopien seriöser Geschäfte. Mit Darstellungen von Produkten, Informationen und falschen Kundenbewertungen sind diese schwer zu erkennen. Als Lockmittel dienen besonders günstige Preise, vor allem von beliebten Produkten, auch dann, wenn die Artikel im Markt gar nicht mehr verfügbar sind. Bestellt eine Kundin oder ein Kunde, bekommt sie oder er entweder minderwertige Ware zu einem überhöhten Preis oder erhält nach einer Vorauszahlung das Produkt gar nicht. Manchmal halten die Kriminellen die Nutzenden mit Lieferschwierigkeiten hin, um sie daran zu hindern, ihre Zahlung rückgängig zu machen. Da die Täterinnen und Täter meist aus dem Ausland agieren, sind diese Fake-Shops schnell mitsamt dem Geld verschwunden und tauchen an anderer Stelle unter neuem Namen wieder auf.

Bitte beachten!

- Bei auffallend günstigen Angeboten sollte man immer auch etwas misstrauisch sein. Seriöse Anbieter sind an der Transparenz ihrer gesetzlichen Pflichtangaben, unabhängigen Warenversicherungen, einer längeren Historie und vor allem am Angebot bekannter zuverlässiger Zahlungsmethoden zu erkennen.
- Für Verkäuferinnen und Verkäufer ist wichtig: Waren sollten nur an vertrauenswürdige Adressen geliefert und verlässliche Zahlungsmethoden, die den Geldeingang garantieren, verwendet werden.
- Sollte es trotz aller Vorsicht doch einmal zu einem Schaden beim Internetkauf kommen, sollte dieser grundsätzlich bei der Polizei angezeigt werden.

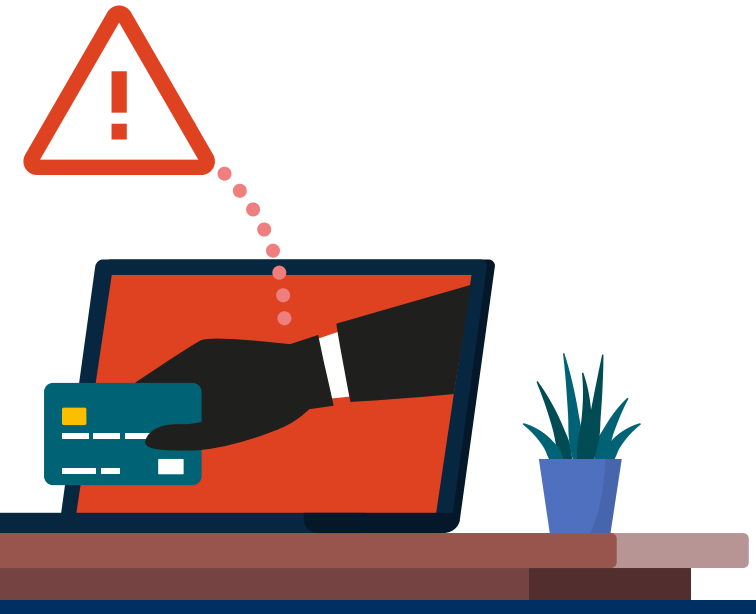
2 TELEFON-SCHWINDEL
MANIPULATION UND TÄUSCHUNG STOPPEN

Social-Engineering

Rund 70 Prozent der Deutschen erledigen gemäß Branchenverband Bitkom ihre Bankgeschäfte online. Sie schätzen den Komfort und die Einfachheit. Die Sicherheit spielt für das Online-Banking eine große Rolle. Banken und Sparkassen haben deshalb keinen Aufwand gescheut, um ausgefeilte Sicherheitsverfahren zu entwickeln und diese stetig zu verbessern. Das beliebte App-basierte SecureGo-Verfahren, das eine Direktfreigabe ohne TAN bietet, oder das auf dem Chip der girocard beruhende SmartTAN-photo-Verfahren sind Beispiele dafür. Ihre Sicherheit wird regelmäßig vom TÜV und anderen Gutachtern bestätigt. So können nur noch Besitzerinnen und Besitzer der zum Konto passenden Sicherheitsmedien Transaktionen durchführen.

Auch Online-Kriminelle haben erkannt, dass sie diese sehr sicheren Systeme nicht knacken können. Sie haben sich deshalb auf eine andere Masche verlegt. Sie greifen Kundinnen und Kunden an, indem sie diese überlisten und ihre Leichtsinnigkeit ausnutzen. Diese Manipulation wird als Social-Engineering bezeichnet. Dabei überreden die Kriminellen Kundinnen und Kunden, betrügerische Transaktionen auszuführen, oder sie überzeugen diese, ihnen sogar eigene Sicherheitsverfahren wie SecureGo oder auch digitale Karten freizuschalten. Mit den Sicherheitsverfahren im Besitz können sie dann in aller Ruhe das Konto der Opfer plündern oder mit der erlangten digitalen girocard oder Kreditkarte selbst auf Shopping-Tour gehen.

Auch wenn viele glauben, dass so eine Manipulation als wenig möglich erscheint: Betrügende schaffen es immer wieder, glaubwürdig zu erscheinen, Kundinnen und Kunden unter Druck zu setzen und dazu zu bewegen, auch Transaktionen freizugeben, die sie eigentlich gar nicht durchführen möchten. Die Kriminellen sprechen in der Regel fließend Deutsch, haben eine geschickte Rhetorik und teilweise auch Faktenwissen, das sie vorher mit Phishing, Diebstahl oder Social-Engineering bei anderen Personen erlangt haben. Immer bessere im Internet verfügbare Stimmsimulatoren helfen ihnen, eine falsche Identität vorzuspielen.



Bitte beachten!

- Lassen Sie sich nicht von fremden Anrufern am Telefon einwickeln, die behaupten, sie wären Bankangestellte, die eine Überweisung wiederholen müssen oder eine Sperrung aufheben wollen, oder aber IT-Techniker, die um eine Testtransaktion bitten oder den PC reparieren wollen.
- Seien Sie grundsätzlich misstrauisch, wenn Anrufe oder Nachrichten angeblich von Ihrer Bank stammen – selbst wenn Telefonnummer oder Absenderadresse seriös erscheinen. Kontaktieren Sie Ihre Bank lieber über die bekannte Hotline oder direkt über Ihr Online-Banking.
- Geben Sie niemals vertrauliche Informationen am Telefon preis. Wenn Sie doch nach solchen Informationen gefragt werden, können Sie mit Sicherheit von einem Betrugsversuch ausgehen und sollten sofort auflegen.

Falsche Anrufe

Beim Enkel- oder Kindertrick treten die Täterinnen und Täter, im Gegensatz zu den zuvor beschriebenen Betrugsarten, oft persönlich beim Opfer auf. Meist melden sie sich vorher per WhatsApp, manchmal auch am Telefon und geben sich als lange nicht gesehene Enkel, Söhne oder Töchter aus. Sie behaupten, eine neue Telefonnummer zu haben und gerade dringend Geld zu benötigen oder ihre Sachen abholen zu wollen. Hier typisch: Die Anrufenden setzen ihr Opfer unter seelischen Druck, schmeicheln sich ein, versuchen mit Annahmen ins Blaue mehr über das Opfer und die finanzielle Situation zu erfahren oder drohen, sonst den Kontakt abzubrechen. Manchmal geben sich die Anrufenden sogar als Polizeibeamte aus, die die Wohnung prüfen oder Wertsachen abholen möchten. Das Ziel dieser kriminellen Kontakte ist, dass das Opfer ihnen Informationen, Wertsachen oder vertrauliche Daten herausgibt. Einige Betrügende begleiten ihre Opfer sogar zum Geldautomaten, damit sie dort zusammen Bargeld für die vorgeblichen Verwandten abholen können.

Die einfachste Möglichkeit, um sich hier abzusichern: auflegen, die WhatsApp-Nachricht löschen und die alte, angeblich nicht mehr gültige Nummer anwählen, um Rücksprache mit den echten Verwandten über den Vorfall zu halten. Auf keinen Fall sollte man unbekannte Personen – nicht einmal kurz – in seine Wohnung lassen.

3 SELBSTSCHUTZ PER SMS-REGEL
SICHER BLEIBEN MIT DREI SCHRITTEN

Die SMS-Regel

Es gibt immer neue Betrugsmaschen. Mit gesundem Menschenverstand und dem Beherzigen von drei einfachen Tipps lassen sich jedoch die meisten Betrugsversuche enttarnen. Gehen Sie nach der sogenannten SMS-Regel vor: **Stoppen – Misstrauen – Schützen.**

Stoppen: Die Betrügenden setzen ihre potenziellen Opfer üblicherweise unter Druck, schnell zu handeln, oder sie bieten verlockende Last-Minute-Angebote an, die angeblich bald ablaufen. So erzeugen sie bei ihren Opfern Stress, um sie unvorsichtig zu machen, und drängen sie zu unbedachten Handlungen. Daher ist es wichtig, erst mal zu stoppen, um Abstand von dem Druck zu gewinnen und sich zu beruhigen, um besonnen handeln zu können.

Misstrauen: Jede Stresssituation sollte man ruhig angehen. So sollte man die Absicht des Gesprächspartners oder der Nachricht hinterfragen und die bestehenden Möglichkeiten überdenken. Fragen Sie sich, warum jemand Sie bedrängt und zur Eile treibt. Woher hat sie oder er Ihre Nummer? Ist der Grund des Anrufs plausibel und wird eine seriöse Telefonnummer angezeigt? Ermöglicht die oder der Anrufende Ihnen einen Rückruf unter einer bekannten, vertrauenswürdigen Telefonnummer? Oder: Warum bietet ein Online-Shop beliebte und stark nachgefragte oder seltene Waren viel billiger an als andere? Trauen Sie sich, wenn Sie Zweifel haben, vertrauenswürdige Personen, wie Freunde, Familie, Ihre Bank oder auch die Verbraucherzentrale zu fragen. Gemeinsam können Sie vermeiden, zum Opfer zu werden.

Schützen: Phishing-E-Mails oder -SMS sollten stets gelöscht, Phishing-Briefe vernichtet und unerwünschte Anrufe sofort unterbrochen werden. Fragen Sie im Zweifelsfall beim Absender direkt nach. Wenn Sie im Internet etwas Auffälliges beobachtet oder einen vermuteten Betrugsversuch abgewehrt haben, melden Sie verdächtige Nutzende an die jeweilige Plattform. So können Sie dazu beitragen, andere zu schützen. Bei wiederholten ungewünschten Anrufen oder falls Sie versehentlich einem Betrug aufgesessen sind, erstatten Sie Anzeige bei der Polizei und übergeben dieser die Phishing-E-Mails oder -Briefe.

Weitere Informationen über sicheres Online-Banking, Online-Shopping sowie einen kostenlosen Internet-Führerschein finden Sie bei „Deutschland sicher im Netz e.V." unter: https://www.sicher-im-netz.de

Herausgeber und verantwortlich für den Inhalt dieser Ausgabe:
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken · BVR, Berlin
Leitung/Chefredaktion: Tim Zuchiatti, BVR – Kommunikation und Öffentlichkeitsarbeit
Autor: Dr. Olaf Jacobsen, BVR
Co-Autor: Dr. Alexander Scheike, BVR
Objektleitung: Manuela Nägel, DG Nexolution eG, Leipziger Str. 35, 65191 Wiesbaden, E-Mail: manuela.naegel@dg-nexolution.de
Verlag und Vertrieb: DG Nexolution eG, vertreten durch den Vorstand: Marco Rummer (Vorsitzender), Dr. Sandro Reinhardt, Florian P. Schultz, Leipziger Str. 35, 65191 Wiesbaden

Gestaltung und Redaktion: hundertzwölf . agentur für kommunikation GmbH, Valentin-Senger-Straße 15, 60389 Frankfurt am Main
Herstellung: Görres-Druckerei und Verlag GmbH, Niederbieberer Str. 124, 56567 Neuwied
Bildnachweis: BVR, iStock