Pressemitteilung

Betrug beim Online-Shopping: Selbst sensibilisierte Verbraucher:innen sind gefährdet

- **Phishing, Smishing und Vishing: Verbraucher:innen geben sensible Daten oftmals unbedacht preis**
- **Weiterhin vermehrt Betrugsversuche über die Plattform Kleinanzeigen**
- **Barclays-Experte Maciej Ewertowski erklärt, wie man sich im Internet am besten schützt**

Hamburg, 7. Juni 2023 – Betrugsversuche auf Verkaufsplattformen im Internet haben weiterhin Hochsaison: Aktuell versuchen Betrüger:innen vor allem die Unbedachtheit von Verkäufer:innen auf dem Portal Kleinanzeigen auszunutzen. Aber auch bei „klassischen" Phishing-Versuchen geben Betroffene oft sensible Daten wie Passwörter, Kreditkartendaten oder mTANs preis oder fallen auf Fake-Webseiten herein. Barclays Experte Maciej Ewertowski möchte Verbraucher:innen sensibilisieren, bei ungewöhnlichen E-Mails, SMS und Anrufen vorsichtig zu sein und appelliert daran, Zahlungsdaten nicht an Dritte weiterzugeben.

„Die Zeiten, in denen vermeintliche Prinzen aus dem Ausland per E-Mail ein Vermögen versprechen und Betrugsversuche leicht zu erkennen waren, sind vorbei. Betrüger zielen heute mit ausgefeilten Social-Engineering-Techniken darauf ab, an geheime Daten zu gelangen oder Zahlungen auszulösen. Selbst vorsichtigen Online-Shopper:innen kann das Schwierigkeiten bereiten", so Maciej Ewertowski, Vice President Fraud Strategy, der bei Barclays Consumer Bank Europe für die Betrugsprävention und -bekämpfung zuständig ist.

Um nicht selbst Opfer von Betrüger:innen zu werden,gibt der Experte Verbraucher:innen folgende Tipps an die Hand:

1) **Fehlerhafte Sprache:** Nachrichten in einer fremden Sprache oder mit auffällig vielen Rechtschreib- und Grammatikfehlern können ein erster Hinweis auf einen Betrugsversuch sein.
2) **Besteht eine Notlage?** Verbraucher:innen sollten misstrauisch sein, wenn in der vermeintlichen Notsituation nur mit Geld geholfen werden kann.
3) **Misstrauen bei Eile:** Wer aufgefordert wird sofort zu handeln und Geld oder Kontodaten zu senden, sollte besonders vorsichtig sein.

4) **Kein Name:** Wenn sich Anrufer:innen am Telefon nicht selbst mit Namen melden, sollten sie dazu aufgefordert werden.
5) **Zu gut, um wahr zu sein:** Wenn Unbekannte ungewöhnlich hohe Zinsen oder Gewinne bei Investitionen versprechen, gilt es, besonders misstrauisch zu sein.

Laut Digitalbarometer 2022 des Bundesamts für Sicherheit in der Informationstechnik ist mehr als jede:r vierte Deutsche schon einmal Opfer von Cyber-Kriminalität geworden (29%).[1] Identitätsdiebstahl, Betrug beim Online-Kauf und Schadsoftware sind dabei die häufigsten Ursachen.

Zahlungen mit Kreditkarte oder über Wallets wie Amazon Pay und Google Pay sind allerdings grundsätzlich sicher, solange Kund:innen diese umsichtig ausführen. „Banken und Zahlungsabwickler betreiben im Hintergrund eine Reihe von Sicherheitsmechanismen, zudem sind die meisten Transaktionen durch die Zwei-Faktor-Autorisierung per Smartphone geschützt. Einen vollständigen Schutz gibt es allerdings nicht. Die größte Sicherheitslücke ist meist der Mensch selbst“, so Ewertowski weiter.

Aktuell viele Phishing-Versuche über Kleinanzeigen
Aktuell werden vermehrt Verkäufer:innen auf der Plattform Kleinanzeigen (ehemals eBay Kleinanzeigen) kontaktiert, um die Kreditkartendaten des Anbietenden zu erschleichen. Die Betrüger fordern Verkäufer:innen auf, die Funktion „Sicher Bezahlen“ für den Verkauf zu nutzen und fragen nach der E-Mail-Adresse. Sie schicken daraufhin eine Phishing-Mail und geben sich als Kleinanzeigen-Kundendienst aus. Die E-Mail soll suggerieren, dass bereits eine Zahlung geleistet wurde. Ein Link in der E-Mail führt dann zu einer betrügerischen Webseite mit der vermeintlichen Zahlungsbestätigung, auf der Verkäufer:innen ihre Kreditkartendaten und anschließend einen Sicherheitscode für den Erhalt des Geldes angeben sollen. Dieser Sicherheitscode wird jedoch genutzt, um eine Zahlung zugunsten des Betrügers auszulösen.

Phishing über Anruf, SMS und WhatsApp
Auch bei Anrufen von unbekannten oder unterdrückten Nummern sollten Verbraucher:innen aufmerksam sein und gegebenenfalls die Telefonnummer

[1] Quelle: Digitalbarometer 2022

mit den Angaben des Unternehmens abgleichen, das der:die Anrufer:in vorgibt zu vertreten.

Betrüger:innen versuchen aber auch weiterhin per SMS und WhatsApp an sensible Kundendaten zu gelangen. Beispiele häufiger SMS sind unter anderem:

- „Ihr Paket kommt an, verfolgen Sie es hier …“
- „Der Artikel, den Sie gekauft haben, wurde geliefert. Bitte überprüfen und akzeptieren Sie ...“

Dafür hat Ewertowski ebenfalls einen Tipp: „Es lohnt es sich, die Einstellungen des Smartphones zu überprüfen. Einige Telefone bieten die Möglichkeit, einen SMS-Spam-Filter einzurichten und betrügerische SMS herauszufiltern.“

Im Notfall schnell die Bank informieren
Wer Opfer eines Betrugs ist oder einen Betrugsverdacht hat, sollte so schnell wie möglich Kontakt mit seiner Bank aufnehmen. Barclays Kund:innen können direkt aus der Barclays App anrufen, sind automatisch legitimiert und erhalten damit schneller Hilfe. Der klassische Anruf über die Hotline oder eine Nachricht über das Postfach in der Barclays App und im Online-Banking sind ebenfalls möglich.

Barclays arbeitet kontinuierlich daran, Betrug durch Kriminelle zu verhindern. Dafür arbeiten automatisierte und komplexe Systeme im Hintergrund. Die Direktbank informiert Kund:innen aber auch plakativ über die App, im Online-Banking oder auf Kontoauszügen. Außerdem werden Kund:innen in Aufklärungskampagnen per E-Mail und über weitere Kontaktpunkte informiert.

***

Hinweis an die Redaktion: Viele weitere Tipps und Details zu aktuellen Betrugsarten finden sich unter https://www.barclays.de/onlinesicherheit/.

Medienkontakt:
Barclays
Consumer Bank Europe

Pressemitteilung

Sascha Nottmeier, Senior Communications Manager
Telefon: +49 151 4126 0082
E-Mail: sascha.nottmeier@barclays.com
www.barclays.de

Über Barclays Consumer Bank Europe:

Barclays ist im Privatkundengeschäft bereits seit mehr als 30 Jahren erfolgreich in Deutschland aktiv und zählt zu den führenden Anbietern von Kreditkarten mit echter Kreditfunktion. Darüber hinaus bietet der Finanzdienstleister Online-Kredite sowie Ratenkauf-Finanzierungen über Amazon.de an. Die Hamburger Niederlassung der Barclays Bank Ireland PLC betreut mit über 700 Mitarbeiter:innen rund 1,9 Millionen Kund:innen. Weitere Informationen finden Sie unter www.barclays.de.