AKTUELLE NACHRICHTEN Österreich
NACHRICHTEN AG
08. Juni 2025

Achtung! Betrüger tarnen sich als A1 und stehlen Kreditkartendaten!

Zunehmende Betrugsversuche im Namen von A1: Kunden werden mit gefälschten SMS über Geschenke und Bonuspunkte getäuscht.

Graz-Umgebung, Österreich - In den letzten Wochen ist eine besorgniserregende Art der Online-Betrugsmasche in Österreich aufgetaucht: Betrüger geben sich als Mitarbeiter des Mobilfunkanbieters A1 aus und informieren Kunden über vermeintlich gesammelte Bonuspunkte. Über SMS werden die Menschen in ein schlüpfriges Spiel gelockt, in dem ihnen ein Geschenk in Aussicht gestellt wird. Um dieses zu erhalten, sollen sie eine Gebühr zahlen. Geht man dem Link in der Nachricht nach, landet man auf einer täuschend echten Kopie der A1-Website, die selbst Experten Schwierigkeiten bereitet, als Fälschung zu erkennen, berichtet meinbezirk.at.

Kunden sind stark unter Druck gesetzt, ihre Kreditkartendaten

anzugeben, mit der Zusicherung, dass alles sicher sei. Doch dieser Druck ist Teil einer fiesen Masche: Nach erfolgreicher Eingabe der Daten versuchen die Betrüger, hohe Beträge von den Konten der Opfer abzubuchen. Guido Zeilinger, ein Konsumentenschützer, warnte vor dieser Art des Betrugs und betonte, dass kein seriöses Unternehmen Portokosten für Geschenke verlangen oder nach Kreditkartendaten inklusive Sicherheitscode fragen würde. Bei Verdacht auf Betrug rät er zu schnellem Handeln: Keinesfalls auf die Aufforderungen reagieren und direkt bei A1 nachfragen.

Phishing: Die Masche hinter dem Betrug

Doch was steckt hinter dieser Betrugsart? Die Methode ist als Phishing bekannt, eine Form des Datenklau, bei der Kriminelle versuchen, persönliche Informationen wie Passwörter und Kreditkartennummern über gefälschte Webseiten, E-Mails oder SMS zu stehlen. Der Begriff leitet sich von „password harvesting“ und „fishing“ ab. Oft sind die fälschenden Nachrichten so gut gemacht, dass sie selbst geübte Nutzer in die Irre führen können, erklärt ndr.de.

Typische Merkmale solcher Phishing-Mails sind fehlende persönliche Anreden, Rechtschreibfehler und manipulative Formulierungen, die zur Eingabe persönlicher Daten auffordern. Besonders überlegen müssen sich Verbraucher, wenn sie unbekannte Absender erhalten: Ein genauer Blick auf den Absender und die Links kann dabei helfen, gefährliche Nachrichten zu identifizieren. Veränderungen der Webseiten, die zu solchen Phishing-Angriffen gehören, sind weitere Alarmzeichen.

Vorbeugen und Handeln bei Verdacht

Was tun, wenn man glaubt, Opfer eines Phishing-Betrugs geworden zu sein? Die Verbraucherzentrale empfiehlt, unverzüglich die Bank zu informieren und Konten zu sperren, um weitere Schäden zu vermeiden. Auch das Löschen der

verdächtigen Nachrichten ist sinnvoll, wobei man diese dennoch als Beweismaterial aufbewahren sollte, wenn man tatsächlich betroffen ist. Ein weiteres Risiko ist das sogenannte SIM-Swapping, bei dem Betrüger die Kontrolle über die Handynummer des Opfers erlangen und so Zugriff auf persönliche Daten erlangen können.

Für den Ernstfall rät die Verbraucherzentrale, auch eine telefonische Beratung in Anspruch zu nehmen. Auf 0900er-Nummern erhalten Betroffene Auskunft zu rechtlichen Fragen und weiteren Schritten. Dieser Beratungsdienst ist nicht nur auf Rechtsfragen beschränkt, sondern kann auch bei finanziellen Angelegenheiten und Produkttests helfen. Die Kosten belaufen sich hier auf etwa 13,70 Euro und werden sekundengenau abgerechnet.

Die Meldung solcher Betrugsmaschen ist wichtig, um weiteren Schaden abzuwenden. Betroffene sollten sich zudem an phishing@verbraucherzentrale.nrw wenden, um die gefälschten Nachrichten zu melden und so zur Aufklärung beizutragen. Angesichts dieser Entwicklungen heißt es für alle: Gut aufpassen und im Zweifelsfall lieber einmal mehr nachfragen.

Wer die Augen offen hält, kann den Betrügern oft einen Strich durch die Rechnung machen.

Details	
Ort	Graz-Umgebung, Österreich
Quellen	• **www.meinbezirk.at** • **www.ndr.de** • **www.vzhh.de**