NACHRICHTEN AG

31. August 2024

Vorsicht Phishing: Comdirect-Kunden müssen jetzt wachsam sein!

Betrüger zielen auf Comdirect-Kunden ab: Phishing-E-Mails entblößen persönliche Daten und leeren Konten. Schützen Sie sich!

Die Gefahren des digitalen Bankings sind nicht zu unterschätzen. Aktuell sollten besonders Kunden der Comdirect-Bank vorsichtig sein. In einer alarmierenden Entwicklung sind verdächtige E-Mails im Umlauf, die darauf abzielen, sensible persönliche Daten zu stehlen. Mit Betreffzeilen wie „Bestätigen Sie Ihre Kontodaten“ erwecken die Nachrichten den Anschein, als kämen sie direkt von der Bank. Einmal geklickt, könnte dies den Verlust von Geld und möglicherweise die Kontrolle über das eigene Konto zur Folge haben.

In Dortmund sind zahlreiche Kunden von dieser fiesen Betrugsmasche betroffen. Cyber-Kriminelle nutzen eine Technik, die als „Phishing“ bekannt ist, um ihre Opfer in die Falle zu locken. Diese Masche funktioniert denkbar einfach: Eine E-Mail fordert den Empfänger auf, sich in sein Online-Banking-Konto einzuloggen und dabei seine Zugangsdaten einzugeben. Ein Klick auf den Link führt zu einer gefälschten Webseite, die jener der echten Bank zum Verwechseln ähnlich sieht, so die Warnungen der Comdirect selbst.

Die Gefahren des Phishings

Der Schlüssel zu diesem Problem ist das „Phishing“, bei dem Kriminelle trickreich versuchen, die privaten Informationen wie Zugangsnummer, PIN und TAN der Kunden zu erlangen. Wer auf

diese Betrüger hereinfällt und diese Daten eingibt, riskiert, dass Täter auf das eigene Konto zugreifen und unautorisierte Transaktionen ausführen. Laut der Verbraucherzentrale lässt sich diese Betrugsform oft an der unseriösen Absenderadresse erkennen; eine richtige Bank würde niemals per E-Mail nach persönlichen Daten fragen.

Ein weiterer Warnhinweis kommt vom Bundesamt für Sicherheit in der Informationstechnik (BSI), das die Gefahren von Phishing klar aufzeigt. Wer beispielsweise seine Kreditkartendaten auf einer gefälschten Webseite eingibt, öffnet Tür und Tor für die Betrüger. Die volkswirtschaftlichen Schäden durch solche Cyber-Delikte, die mit Phishing-Attacken beginnen, belaufen sich in Deutschland jährlich auf mindestens einen zweistelligen Millionenbetrag. Dies verdeutlicht die Dringlichkeit, sich effektiv vor solchen Angriffen zu schützen.

Präventionsmaßnahmen für Bankkunden

Um sich effektiv gegen Phishing-Angriffe zu wappnen, wird empfohlen, verdächtige E-Mails unverzüglich in den Spam-Ordner zu verschieben. Ein einfacher Trick kann auch helfen, die Sicherheit zu erhöhen: Kunden können ihren Mauszeiger über Links in E-Mails bewegen, um die tatsächliche URL anzuzeigen, bevor sie darauf klicken. Diese Maßnahme bietet eine zusätzliche Schutzebene, indem sie auf einen Blick zeigt, ob die E-Mail wirklich von der Bank oder von Betrügern stammt. Allerdings funktioniert dieser Trick bisher nur auf Desktop-Computern und nicht auf Mobilgeräten.

Es ist erwähnenswert, dass Betrüger nicht nur E-Mails versenden. Jüngste Berichte zeigen, dass sie sich auch als seriöse Banken in Briefen ausgeben, um noch mehr Menschen zu täuschen. Diese Vorfälle haben gezeigt, dass selbst gut gemeinte Sicherheitsmaßnahmen nicht ausreichen. Es bleibt entscheidend, wie Benutzer auf diese Warnungen reagieren und ob sie ihre digitalen Bankgeschäfte mit größter Vorsicht und Wachsamkeit angehen. Die Gefahr ist real, und wie die

Erfahrungen der Comdirect-Kunden zeigen, sollten wir alle sorgfältig mit unseren persönlichen Daten umgehen.

Details