NACHRICHTEN AG

31. August 2024

Vorsicht, Comdirect-Kunden: Neue Phishing-Mails im Umlauf!

Betrüger zielen auf Comdirect-Kunden ab: Phishing-Mails riskieren Kontoleerung. Schützen Sie Ihre Daten jetzt!

Unsichere Zeiten für Bankkunden: Betrüger sind aktiv und haben es erneut auf die persönlichen Daten der Comdirect-Kunden abgesehen. Eine aktuelle Phishing-E-Mail mit dem Betreff „Bestätigen Sie Ihre Kontodaten“ könnte für viele zur Falle werden. Kunden werden dringend gewarnt, diese Nachrichten nicht zu beantworten und sofort in den Spam-Ordner zu verschieben.

In Dortmund sind bereits zahlreiche Berichte über derartige betrügerische Aktivitäten eingegangen. Die Comdirect-Bank selbst hat ihre Nutzer auf ihrer Website davor gewarnt, dass Cyber-Kriminelle versuchen, durch täuschend echte E-Mails ihre persönlichen Daten zu ergaunern. Bei Phishing handelt es sich um eine Methode, bei der Kriminelle durch gefälschte E-Mails die Empfänger dazu bringen, vertrauliche Informationen preiszugeben, etwa durch den Login in ein gefälschtes Bankkonto.

Wie funktionieren Phishing-Attacken?

Phishing-E-Mails stellen oft eine gefährliche Masche dar, die auf den ersten Blick harmlos erscheinen mag. In der Regel enthalten sie einen Link, der zu einer nachgebauten Webseite führt, die der echten Online-Banking-Seite zum Verwechseln ähnlich sieht. Wenn Kunden bereitwillig ihre Zugangsdaten wie PIN oder TAN eingeben, können die Betrüger sofort auf deren Konten

zugreifen und unautorisierte Transaktionen durchführen.

Die Verbraucherzentrale weist darauf hin, dass jeder Bankkunde sehr vorsichtig sein sollte, insbesondere wenn verdächtige Absenderadressen benutzt werden. „Eine seriöse Bank würde niemals über E-Mail um persönliche Daten bitten“, erklärt ein Sprecher der Verbraucherzentrale. Daher ist es ratsam, solche Mails direkt als Spam zu kennzeichnen. Ein einfaches „Mouseover“ über den Link in der E-Mail kann oft schon helfen, die wahre URL zu überprüfen, die angezeigt wird, wenn man mit der Maus über den Link fährt. Auf Mobilgeräten funktioniert dies allerdings nicht.

Die Gefahren durch solche Cyber-Attacken sind gravierend. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits erklärt, dass die volkswirtschaftlichen Schäden durch Phishing-Angriffe in Deutschland auf einem zweistelligen Millionenbetrag jährlich geschätzt werden. Bei der aktuellen Welle von Angriffen, nicht nur auf Comdirect, sondern auch auf andere Banken, ist höchste Vorsicht geboten.

Was tun im Ernstfall?

Kunden, die versuchten, sich in ihr Online-Banking-Konto einzuloggen und das Gefühl haben, dass ihnen eine gefälschte Seite untergejubelt wurde, sollten direkt handeln. Es ist entscheidend, in solchen Fällen die Bank zu kontaktieren. Die Bank kann dann prüfen, ob es tatsächlich unautorisierte Zugriffe auf das Kundenkonto gab und gegebenenfalls Maßnahmen ergreifen.

Um auf der sicheren Seite zu sein, ist es auch klug, regelmäßige Kontenabgleiche vorzunehmen und seine Bankinformationen stets im Auge zu behalten. So können Kunden schneller reagieren, sollte es zu verdächtigen Aktivitäten kommen.

Besonders in der heutigen digitalen Welt ist es wichtig, die eigenen Daten gut zu schützen und stets wachsam zu bleiben.

Scams werden immer raffinierter und die Betrüger geben sich Mühe, potentielle Opfer in ihre Netzwerke zu ziehen. Daher ist die Aufklärung über solche Risiken und die Einhaltung von Sicherheitsstandards entscheidend, um finanzielle Verluste zu vermeiden.

In der aktuellen Situation ist es von Bedeutung, sich nicht nur auf technische Schutzsysteme zu verlassen, sondern auch das eigene Bewusstsein für mögliche Bedrohungen zu schärfen.

Details