



**Pressemitteilung der Union
Luxembourgeoise des
Consommateurs**



(Lëtzebuenger Konsumenteschutz)

Phishing-Angriffe: ULC sieht vor allem Banken in der Pflicht

Die Zahl der Phishing-Angriffe ist im vergangenen Jahr geradezu explodiert. 2023 wurden in Luxemburg offiziell mehr als 1.300 solcher Betrugsfälle registriert. Wie hoch die Dunkelziffer ist, ist schwer zu sagen, da viele Opfer solche Angriffe – oft aus falscher Scham – nicht anzeigen. In Anbetracht der zunehmenden Bedrohung durch Phishing und Internetkriminalität möchte die Union Luxembourgeoise des Consommateurs (ULC) am heutigen Safer Internet Day an die Verantwortung der Verbraucher, des Gesetzgebers, aber vor allem an jene der Banken erinnern, deren Kunden besonders oft Ziel von Cyberkriminellen sind.

Betrügerische Akteure nutzen immer raffiniertere Taktiken, um persönliche Daten und finanzielle Informationen von ahnungslosen Opfern zu stehlen. Als Verbraucher sollte man daher niemals persönliche oder finanzielle Informationen über unsichere Kanäle preisgeben. Bei unerwarteten E-Mails, Nachrichten oder Anrufen, die einen dazu auffordern, sensible Daten wie Passwörter, Kontonummern oder Sozialversicherungsnummern preiszugeben, sollte man immer misstrauisch sein. Ein gesundes Maß an Skepsis kann helfen, Phishing-Angriffe frühzeitig zu erkennen und zu vermeiden. Eine hundertprozentige Garantie ist dies aber nicht – vor allem nicht in Zeiten, in denen sogar staatliche Accounts wie LU-Alert von SMS-Betrügnern missbraucht werden.

Apropos Staat: Wenn man den digitalen Wandel vorantreiben will, ohne dabei das Vertrauen der Verbraucher aufs Spiel zu setzen, müssen diese besser geschützt werden. Öffentliche Aufklärungskampagnen sowie die Arbeit von Bee Secure und Co. sind sicher ein guter Anfang. Es braucht aber vor allem schärfere Gesetze und Vorschriften und eine konsequentere Strafverfolgung sowie angemessene Sanktionen, wenn man den Kampf gegen Internetbetrüger nicht verlieren will. Da Phishing-Netzwerke oft grenzüberschreitend agieren, muss auch die internationale Zusammenarbeit zwischen Regierungen und Strafverfolgungsbehörden verbessert werden.

„Eine besondere Verantwortung beim Thema Phishing kommt definitiv den Banken zu. Durch immer weniger Service und immer mehr Filialschließungen zwingen die Geldinstitute viele Verbraucher geradezu zum Online-Banking – vor allem, aber nicht nur solche, die wenig internetaffin sind“, so ULC-Präsident Nico Hoffmann.

Die Banken spielen eine entscheidende Rolle beim Schutz ihrer Kunden vor Phishing-Angriffen. Sie müssen ihre Kunden nicht nur laufend über die neuesten Phishing-Methoden und Betrugsmaschen auf dem Laufenden halten, sondern ihre Kunden auch bestmöglich vor Betrug schützen, um sicherzustellen, dass nur autorisierte Benutzer auf Konten zugreifen

können. „Die Kunden zum Umstieg vom gewohnten Token zu einer Smartphone-abhängigen und damit deutlich teureren Lösung zu zwingen, kann auf jeden Fall nicht die Antwort auf alle Sicherheitsfragen sein“, so Nico Hoffmann.

Gefordert sind die Banken insbesondere dann, wenn einer ihrer Kunden Opfer eines Phishing-Angriffs geworden ist. In den meisten Fällen versuchen die Banken, ihren Kunden den Schwarzen Peter zuzuschieben, indem sie ihnen grobe Fahrlässigkeit vorwerfen, um sich so vor der Erstattung gestohlener Gelder zu drücken. Dazu Nico Hoffmann: „Anstatt Opfer von Cyberkriminalität zu stigmatisieren, sollten Geldinstitute ihren Kunden in solchen Situationen zur Seite stehen und Verantwortung übernehmen. Schließlich kann jedermann Opfer einer dreisten Betrugsmasche werden. Wie sonst lässt es sich erklären, dass selbst Bankangestellte – also Profis – hin und wieder auf Online-Betrüger hereinfliegen?“

Mitgeteilt von der ULC am 6.2.2024