Sparkasse Gladbeck

Pressemitteilung vom 25.06.2021

Achtung! Vermehrte Cyberangriffe und andere Betrugsmaschen

So schützen sich Sparkassen- und Bankkunden vor Kriminellen

Ein Albtraum: Betrüger gelangen an Ihre Kontodaten und können Ihr gesamtes Geld abbuchen. Ob durch Phishing, Fake-Shops oder Viren - ein falscher Klick kann enormen Schaden verursachen. Die Tricks der Kriminellen werden immer raffinierter und finden sowohl online als auch offline statt. Wir klären Sie über häufige Betrugsmaschen auf – damit Sie Datendieben auf die Schliche kommen.

Das Wichtigste in Kürze:

- Ignorieren Sie E-Mails und SMS von unbekannten Absendern. Seien Sie misstrauisch, wenn Sie angeblich von Ihrer Sparkasse oder anderen Unternehmen aufgefordert werden, einen Link anzuklicken, um dann auf einer Website sensible Daten einzugeben.
- Fallen Sie nicht auf Anzeigen von Trading-Portalen rein, die mit enormen Gewinnen bei Geldanlagen locken.
- Mitarbeiter in Banken und Sparkassen fragen niemals am Telefon nach PINs, TANs oder Passwörtern.
- Seien Sie skeptisch, wenn sich jemand als Verwandter von Ihnen ausgibt und um Geld bittet.
- Prüfen Sie Ihre Post genau und senden Sie niemals vertrauliche Unterlagen an eine andere Adresse als die Ihrer Bank oder Sparkasse.
- Achten Sie immer darauf, keine sensiblen Daten lesbar in den Papiermüll zu schmeißen.

Laut dem Cybercrime-Lagebericht 2020 des Bundeskriminalamts (BKA) stieg die Cyber-kriminalität um 8 Prozent im Vergleich zum Vorjahr. Kriminelle haben die Ausnahmesituation der Pandemie gezielt ausgenutzt, um Internetnutzer vermehrt auf betrügerische Links zu

locken. Zwar sind einige Angriffsformen seit Jahren bekannt; sie werden aber ständig den neuen technischen Entwicklungen angepasst und bleiben dadurch gefährlich.

Hinzu kommt: Datendiebe nutzen auch häufig analoge Betrugsmaschen, um so dem immer sicherer werdenden digitalen Datenverkehr entgegenzuwirken.

1. Der Betrugsklassiker: Phishing

Beim Phishing verschicken Betrüger in großem Stil E-Mails oder auch SMS, die so aussehen als kämen sie von Unternehmen wie beispielsweise Amazon, Ihrem Telefonanbieter oder Ihrer Sparkasse. Die dringend klingende E-Mail lockt Sie über einen Link auf eine täuschend echt aussehende Kopie der originalen Website. Auf der manipulierten Seite sollen Sie dann Ihre Kontodaten samt Passwort oder Geheimzahl eingeben. Vermeintlich, um Ihr Konto wieder freizuschalten. Stattdessen erbeuten die Datendiebe hochsensible Informationen.

Laut BKA ist das durchschnittliche Spam-Mail-Aufkommen in 2020 um 17 Prozent gegenüber dem Vorjahr gestiegen. Doch keine Sorge: Hier finden Sie umfassende Infos, wie Phishing funktioniert und wie Sie betrügerische Mails oder SMS erkennen können. Denn der beste Schutz sind Aufklärung und ein gesundes Misstrauen.

2. Betrügerische Online-Trading-Portale

Dieser Betrug hat in den vergangenen Monaten an Fahrt aufgenommen: Gefakte Anzeigen – teils sogar mit Prominenten – werben mit enormen Gewinnen bei Geldanlagen wie Kryptowährungen. Der Link führt dann auf eine gefälschte Online-Trading-Website.

Nach der Registrierung bekommen die Nutzer Anrufe eines angeblichen „Brokers“ oder persönlichen „Anlageberaters“. Dieser versucht, den Anleger zu immer größeren Investitionen zu überreden – um angeblich noch höhere Gewinne zu erzielen. Durch die teils regelmäßigen Anrufe wird ein persönlicher Kontakt oder gar eine Vertrauensbeziehung aufgebaut. Dahinter steckt jedoch professioneller Cyberbetrug.

3. Der Fake-Sparkassen-Berater

Ihren Haus- oder Wohnungsschlüssel würden Sie niemals an unbekannte Dritte weitergeben. Schließlich hätten diese dadurch Zugriff auf alle Besitztümer in Ihrem Zuhause. Gleichen Wert haben TANs und PINs, die Ihr Konto und damit Ihr Geld schützen. Da gerade jetzt während der Corona-Pandemie viele Unternehmen und Kreditinstitute auf andere Kommunikationswege setzen, satteln auch die Betrüger um und versuchen, als falsche Sparkassen-Mitarbeiter per Telefon sensible Daten zu ergaunern. Meist rufen sie außerhalb der Öffnungszeiten an und geben vor, es besonders eilig zu haben, weil sonst beispielsweise das Konto gesperrt werden müsse.

Mitarbeiter von Banken und Sparkassen würden jedoch niemals am Telefon nach PINs, TANs oder Passwörtern fragen. Legen Sie im Zweifel einfach auf und rufen Sie Ihre Sparkasse unter der Ihnen bekannten Rufnummer zurück – so können Sie in Erfahrung bringen, ob wirklich Handlungsbedarf besteht. Ein echter Sparkassen-Mitarbeiter hat mit diesem Vorgehen auch kein Problem.

Wichtig: Die Betrüger können auch die Rufnummer fälschen, die Ihnen im Display angezeigt wird. Wenn Sie jedoch auflegen und selbst noch mal die Nummer Ihrer Sparkasse wählen, landen Sie auch sicher dort. Und: Lassen Sie sich niemals unter Zeitdruck zu irgendwelchen Handlungen zwingen.

4. Der Enkeltrick

Der Begriff „Enkeltrick“ wird Ihnen sicherlich schon einmal begegnet sein. Seit Jahrzehnten geben sich Betrüger am Telefon als Verwandte aus, die dringend Geld benötigen. Besonders häufig sind davon ältere Menschen betroffen, die gutgläubig Hilfe anbieten und sich über jeden Anrufer freuen. Dabei wird diese Gutmütigkeit schamlos ausgenutzt. Auch wenn Sie selbst davon nicht betroffen sind, sollten Sie darauf achten, dass in Ihrem familiären oder freundschaftlichem Umfeld niemand Opfer der Betrugsmasche wird.

5. Die „Back-to-the-roots“-Briefpost

Briefe sterben aus – würde man meinen. Aber viele wichtige Unterlagen müssen auch im Jahr 2021 noch per Post geschickt werden – das gilt auch für Schreiben von Banken und Sparkassen.

Seien Sie skeptisch, sobald Sie in einem Brief aufgefordert werden, sensible Unterlagen zu versenden. Achten Sie beispielsweise auf die Empfängeradresse: Ist das die Anschrift Ihrer Sparkasse? Falls nicht, sollten Sie vorsichtig sein. Fragen Sie im Zweifel lieber einmal mehr nach, ob es sich hierbei tatsächlich um ein Schreiben Ihres Instituts handelt. Oder werfen Sie die geforderten Unterlagen einfach selbst in den Briefkasten Ihrer Filiale.

6. Die menschlichen Waschbären

Durch das Homeoffice kann es passieren, dass vertrauliche Informationen versehentlich im hauseigenen Papiermüll landen, die eigentlich in die Aktenvernichtung im Büro gehören. Selbst wenn Betrüger nicht zwangsläufig anfangen, wie Waschbären in Ihren Mülltonnen herumzukramen, kann es passieren, dass unfreiwillig sensible Daten in die falschen Hände geraten. Man weiß schließlich nie, durch wessen Hände der Papiermüll genau geht und welche neuen Ideen Datendiebe als nächstes haben. Achten Sie unbedingt beim Sortieren Ihrer Unterlagen darauf, was genau im Müll landet und ob man dies nicht besser geschwärzt oder geschreddert entsorgen sollte.

Was tun, wenn ich auf eine Betrugsmasche reingefallen bin?

Das Wichtigste ist: Ruhe bewahren. Wenden Sie sich an Ihre Sparkasse, schildern Sie möglichst genau, was passiert ist und welche Daten Sie herausgegeben haben. Die Beraterinnen und Berater werden dann umgehend Erste Hilfe leisten und beispielsweise das Online-Banking sperren oder einen Überweisungsrückruf beauftragen. Sinnvoll ist es auch, bei der Polizei Anzeige zu erstatten – es handelt sich hierbei ganz klar um eine Straftat. Sie können sich sicher sein, dass Ihre Sparkasse Sie bei allem, was zu tun ist, unterstützen wird.

Good to know:

Sollten Sie auf eine Betrugsmasche aufmerksam werden – sei es analog oder digital – können Sie hier Hilfe finden. Ihr Computer-Notfallteam der Sparkassen Finanzgruppe informiert über aktuelle Sicherheitswarnungen und nimmt sich Ihrer an. Verdächtige Nachrichten können Sie zur Bewertung und zum Schutz anderer Kunden an warnung@sparkasse.de weiterleiten.

Ihr Ansprechpartner bei Rückfragen:

Mathias Bludau

Vorstandunterstützung
Referent Marketing / Öffentlichkeitsarbeit
Sparkasse Gladbeck

Telefon 02043 271-343
Telefax 02043 271-266
Mail: mathias.bludau@sparkasse-gladbeck.de