

PRESSEMITTEILUNG

Günzburg, 22. März 2023

Vorsicht, Betrug! Warum sicheres Online-Banking trotzdem möglich ist.

Aus aktuellem Anlass informiert die Sparkasse Günzburg-Krumbach über derzeit laufende Betrugsversuche in Verbindung mit dem Online-Banking und bietet Tipps zur Vermeidung von Schäden.

Sie erhalten eine SMS, in der Sie aufgefordert werden, aufgrund des angeblichen Ablaufs Ihrer Online-Banking-Registrierung einen Link anzuklicken, Daten einzugeben sowie eine Freigabe in Ihrer Banking-App durchzuführen. Sie lesen eine an Sie adressierte E-Mail mit dem Betreff "Sparkasse: Wichtige Interaktion erforderlich", in der Sie gebeten werden, einen Button anzuklicken, um eine eingehende Zahlung zu bestätigen. Ein/e vermeintliche/r Sparkassenmitarbeiter*in ruft Sie an und möchte sensible Daten (z. B. Zugangsdaten oder Geheimzahlen) in Erfahrung bringen. Wie reagieren Sie in diesen Fällen richtig?

Sie und Ihr Vermögen zu schützen liegt Ihrer Sparkasse sehr am Herzen. Aktuell sind leider vermehrt betrügerische Aktivitäten wie die oben beschriebenen zu verzeichnen. Ist Ihr **Online-Banking** trotzdem **sicher**? **Ja**, dafür sorgen **zahlreiche Sicherheitsfaktoren**, wie zum Beispiel der Einsatz von höchsten Verschlüsselungs-Standards bei den Banking-Seiten oder -Apps der Sparkassen sowie die Umsetzung einer Zwei-Faktor-Authentifizierung durch die notwendige Eingabe von Transaktionsnummern bei bestimmten Vorgängen.

Warum kann es trotzdem zu Schäden kommen? Weil Betrüger den „Faktor Mensch“ nutzen, um an Ihre Zugangsdaten oder andere sensible Informationen zu kommen. Deshalb gilt: Online-Banking ist sicher – wenn Sie ein paar wichtige Regeln beachten.

Der wichtigste Hinweis überhaupt: Ihre Sparkasse wird Sie niemals per E-Mail, SMS oder Anruf dazu auffordern, vertrauliche Daten wie PIN, TAN oder Kontonummer bekannt zu geben. Ignorieren Sie solche Versuche am besten komplett, klicken Sie auf keinen Fall Links in E-Mails oder in SMS-Nachrichten an und legen Sie bei dubiosen Anrufen einfach auf.

Zudem sollten Sie Ihre Zugangsdaten sorgfältig auswählen und vorsichtig damit umgehen. Wählen Sie ein sicheres, komplexes Passwort für Ihren Online-Zugang und speichern Sie dieses nirgendwo ab. Sperren Sie außerdem Ihren Online-Banking-Zugang umgehend, wenn Ihnen etwas verdächtig vorkommt. Prüfen Sie auch regelmäßig Ihre Kontobewegungen.

In unserer Internet-Filiale unter dem Link www.spk-gz-kru.de/sicherheit werden laufend aktuelle Sicherheitswarnungen des Computer-Notfallteams der Sparkassen-Finanzgruppe sowie Informationen zu häufigen Betrugsmaschen für Sie bereitgestellt. Unter www.bsi.de finden Sie darüber hinaus weitere hilfreiche Hinweise des Bundesamtes für Sicherheit in der Informationstechnik.

Sollten Fragen aufkommen oder sollten Sie aktuell von einem Betrugsversuch betroffen sein, kommen Sie gern unter 08221 92-0 auf Ihre Sparkasse zu.



Foto: Demet Karatas (Sparkasse)

Pressekontakt:
pressestelle@spk-gz-kru.de
Tel. 08221-92 1010
www.spk-gz-kru.de