Geben Sie Internet-Betrügern keine Chance!

Bitte nehmen Sie sich ein paar Minuten Zeit. Wir informieren über Betrugsversuche und Schutzmaßnahmen. Übrigens finden Sie auf der Rückseite den Kurz-Überblick für unterwegs.

1. Fallen Sie nicht auf die derzeit aktuellen Betrugsmethoden rein!

Ist Ihr PC mit einem sogenannten „Echtzeit-Trojaner“ infiziert, kann dadurch Ihr Online-Banking manipuliert werden. Sie werden auf eine Seite gelockt, die der Original-Seite zum Verwechseln ähnlich sieht. Mit der Anmeldung zum Online-Banking werden Ihre Dateneingaben mitgelesen. Danach erfolgt zum Beispiel die Aufforderung zu

- einer Sicherheits-, Konto-, Software- oder pushTAN-Aktualisierung
- Einführung neuer Sicherheitsstandards oder entsprechender Updates
- der Durchführung einer Demo- oder Testüberweisung
- der Rücküberweisung eines angeblich versehentlich auf Ihr Konto erfolgten Zahlungseingangs, wobei Ihnen u. U. ein entsprechender Zahlungseingang vorgegaukelt wird

Teilweise werden diese Methoden mit einer angeblichen Kontosperre oder dem **Anruf eines angeblichen Sparkassen-Mitarbeiters** kombiniert. Parallel missbrauchen die Betrüger Ihre eingegebenen Daten, um damit eine tatsächliche Überweisung von Ihrem Konto auszuführen.

Betrüger geben sich telefonisch auch als **Supportmitarbeiter von Microsoft, Apple oder anderen namhaften Unternehmen** aus, die Ihren angeblich infizierten Rechner per Fernwartung kostenpflichtig bereinigen wollen und erheblichen Druck aufbauen. Häufig sollen Sie den Aufwand durch den Erwerb von Gutscheinen bezahlen.

Auf unserer Website erhalten Sie unter „Aktuelle Sicherheitswarnungen“ ausführliche Beschreibungen. Entdecken Sie derartige oder ähnliche Auffälligkeiten an Ihrem PC, informieren Sie uns telefonisch oder per E-Mail: 02451 600 oder info@kskhs.de

2. Prüfen Sie die Anzeige auf Ihrem Handy, Smartphone oder dem TAN-Generator sorgfältig

Bevor Sie eine TAN eingeben, prüfen Sie immer sorgfältig, ob die Anzeige im Display Ihres Gerätes tatsächlich den Daten entspricht, die Sie zuvor selber in der Überweisung eingegeben haben bzw. Ihrem Auftrag entspricht. Geben Sie nur eine TAN ein, wenn SIE eine Zahlung oder die Digitalisierung Ihrer Karte veranlassen wollen. Seien Sie besonders wachsam, wenn Sie irgendwelche „Codes“ bestätigen sollen. Im Zweifel brechen Sie die Transaktion sofort ab und informieren uns.

3. Das offene Schlosssymbol zeigt eine unsichere Eingabe. Nutzen Sie den Browser „S-Protect“.

Achten Sie beim Online-Banking stets auf das Schlosssymbol im Browser. Ist es nicht geschlossen oder fehlt es, brechen Sie Ihre Transaktion sofort ab und informieren Sie uns. Sie können auch den sicheren Browser „S-Protect“ für Ihr Banking nutzen, den Sie kostenlos erhalten.

4. Kontrollieren Sie regelmäßig und zeitnah Ihre Kontoumsätze.

Damit Sie unberechtigte Buchungen rechtzeitig erkennen, prüfen Sie regelmäßig Ihre elektronischen Konto- oder Papierauszüge. Der Kontowecker hilft Ihnen dabei. Innerhalb des Online-Bankings finden Sie unter „Einstellungen“/ “Finanzplaner & Zusätzliche Dienste“/ „Kontowecker“ den Kontostands-, Umsatz- und Limit-Wecker. Dort können Sie alles nach Ihren Bedürfnissen einstellen.

5. Begrenzen Sie Ihr Online-Banking-Tageslimit.

Die Wahl eines angemessenen Tageslimits trägt zur Risiko-Minimierung bei. Nutzen Sie das Online-Banking ohne eine Banking-App oder Banking-Software, empfehlen wir Ihnen ein Limit von max. 10.000,00 Euro.
Umbuchungen zwischen Ihren eigenen Konten, dem Eheleute-Konto und den Konten Ihrer minderjährigen Kinder können Sie unabhängig vom Tageslimit in unbegrenzter Höhe ausführen. Den Kreis der Kontoinhaber können Sie dafür durch die Zusatzvereinbarung „Komfortüberweisung“ erweitern. Fragen Sie Ihren Berater.

Reduzieren Sie Ihr Limit am besten sofort online.

Benötigen Sie regelmäßig ein Tageslimit über 10.000,00 Euro empfehlen wir die Abwicklung ausschließlich über eine Banking-Software, z. B. SFirm, mit Sparkassen-Card & USB-Lesegerät.

6. Schützen Sie Ihren PC und Ihr Handy vor ungebetenen Gästen.

„Türsteher", wie eine Personal-Firewall und ein Virenscanner, helfen Ihnen dabei. Beides sollten Sie täglich aktualisieren. Ebenso wichtig ist die permanente Installation von Sicherheitsupdates und Service Packs zu Ihrem Betriebssystem (z. B. Windows), Ihrem Internet-Browser (z. B. Internet Explorer, Firefox), Adobe Reader, Media Player. Aktivieren Sie automatische Updates. Überprüfen Sie Ihren Rechner regelmäßig auf Befall. Unter www.botfrei.de finden Sie Tipps, Anleitungen und einen Cleaner.

7. Denken Sie an Ihre Diskretion. Nutzen Sie den Passwort-Manager „S-Trust".

Ihre Zugangsdaten zum Banking und anderen Accounts sowie andere persönliche Daten sind nur für Sie bestimmt. Verzichten Sie auf die Eingabe persönlicher Daten, wie z. B. die Nummer Ihrer Kredit-/Sparkassen-Card, Ihres Smartphones/Handys, in irgendein Internet-Formular. Geben Sie niemals Ihre Unterschrift, Ihren Personalausweis oder Ihre Lohn- und Gehaltsabrechnung in gescannter Form weiter, auch nicht als Upload. Unter www.s-trust.de finden Sie den Dokumenten- und Passwort-Manager der Sparkasse.

8. Prüfen Sie E-Mails, Links und Downloads kritisch.

Öffnen Sie nicht jeden E-Mail-Anhang und klicken Sie nicht auf jeden Link, der in einer Mail angegeben wird. Die E-Mails stammen nicht unbedingt von dem Absender, der auf den ersten Blick erkennbar ist. Durch einen knackigen Betreff versuchen Betrüger zunächst, Ihre Neugier zu wecken, Ihnen Angst einzujagen, Ihre Hilfsbereitschaft auszunutzen oder Sie mit verlockenden Versprechen zu ködern. Haben Sie z. B. keine elektronische Rechnung mit dem angeblichen E-Mail-Versender vereinbart, ignorieren Sie derartige Mails. Betrüger verstecken im Anhang oder dem Link häufig eine Schadsoftware („Trojaner"), die sich mit dem Start unbemerkt auf Ihrem Rechner installiert. Die Falle schlägt sofort oder mit zeitlicher Verzögerung zu. Hinterfragen Sie im Zweifel beim angeblichen Absender die Richtigkeit, bevor Sie einen unüberlegten Klick machen.
Leiten Sie uns bitte „Sparkassen-Spam-Mails" formlos an „warnung(at)sparkasse.de" weiter.

9. Bleiben Sie aufmerksam und misstrauisch und fragen Sie im Zweifel Ihren Berater.

Kommt Ihnen etwas seltsam vor, brechen Sie die Transaktion ab. "Hören Sie auf Ihren Bauch." Lassen Sie sich nicht unter (Zeit-)Druck setzen.

10. Im Notfall: Sperren Sie Ihren Online-Banking-Zugang.

Dazu

- rufen Sie Ihren Berater, unser Service-Center (02451 600) oder 116 116 an
- oder Sie sperren Ihren Zugang selber sofort: Geben Sie 3 x eine falsche PIN ein!
- Prüfen Sie Ihren PC auf Befall und löschen Sie gefundene Schädlinge, z. B. mit Cleanern von www.botfrei.de

Zum Ausschneiden:

Einfach immer dabei:

Die 10 Kernregeln für sicheres Online-Banking

Für Mobile Banking und Apps halten wir weitere Tipps für Sie bereit!

Stand 01/2023

Aktuelle Sicherheitswarnungen und Hinweise finden Sie:
auf unserer Website, z. B.
- Sicherheitskontrolle
- Konto-/Softwareaktualisierung
- Demo-/Testüberweisung
- Zahlung-Rücküberweisung
- Microsoft-/Apple-Anrufe

Tipps & Cleaner: www.botfrei.de

Im NOTFALL
Sperre 116 116 oder
3 x falsche PIN eingeben, ggf. von anderem PC

Prüfen Sie immer:
- Displayanzeige am Smartphone/TAN-Generator
- Schlosssymbol im Browser
- Kontoumsätze/Kontowecker
- Firewall, Virenscanner aktiv?
- Werden alle Sicherheitsupdates automatisch aktualisiert?

Wichtig:
- Vorsicht beim Öffnen von: E-Mail-Anhängen & Links
- Geben Sie keine persönlichen Daten weiter.
- Wählen Sie Ihr OB-Limit nicht zu hoch.