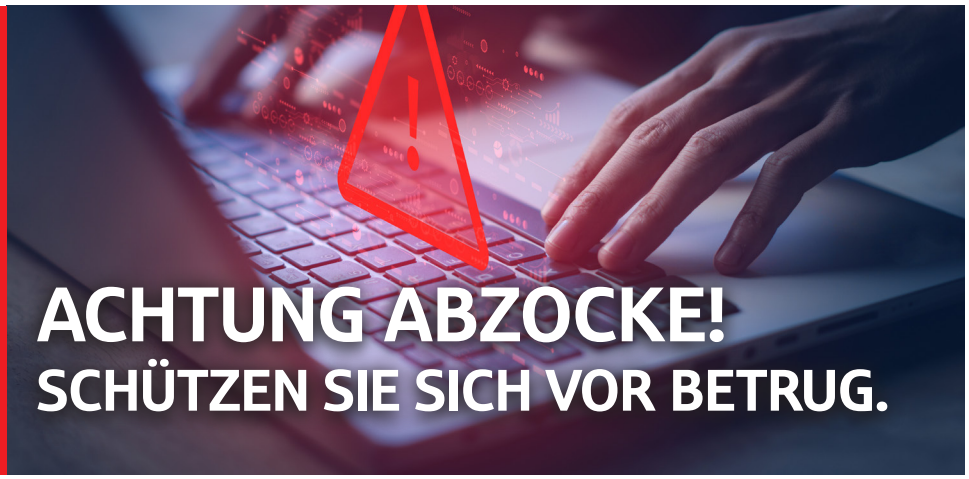
Sparkasse
Neumarkt-Parsberg



ACHTUNG ABZOCKE!
SCHÜTZEN SIE SICH VOR BETRUG.

In der heutigen Zeit sind Daten sehr wertvoll. Kriminelle versuchen, Menschen um ihr Geld oder ihre Wertgegenstände zu bringen.

Es ist extrem wichtig, sich vor Betrug zu schützen und sicherzustellen, dass weder Sie noch Ihre Angehörigen Opfer werden.

Um Sie dabei zu unterstützen, haben wir einige wichtige Informationen zusammengestellt, die verdeutlichen, wie Sie sich vor den gängigsten Betrugsmaschen schützen können.

Technik:
Selbstverständlich erfüllen wir die gesetzlichen und regulatorischen Anforderungen an ein **modernes** und **sicheres Online- und Mobile-Banking.** Wir investieren kontinuierlich in die **neueste Technik und Sicherheitsmaßnahmen.** Wichtig ist daher vor allem Ihre Wachsamkeit!

Psychologische Tricks:
Kriminelle versuchen Sie unter psychologischem Druck und einem Vorwand dazu zu verleiten, etwas zu tun, **was Sie normalerweise nie tun würden. Die Schwachstelle sind also Sie. Gleichzeitig** sind Sie das **Sicherheitsschloss,** wenn Sie aufmerksam, sensibel und **vorsichtig** sind und die **jeweilige Situation kritisch hinterfragen.**

Die am weitesten verbreiteten Betrugsmaschen sind:

- → **Phishing-Angriffe**
- → **Microsoft-Betrug**
- → **WhatsApp-Betrug**
- → **Kleinanzeigen-Betrug**

Diese Betrugsmaschen werden regelmäßig angepasst oder leicht verändert und jeden Tag fallen Menschen darauf herein. **Sorgen Sie dafür, nicht zu den Opfern zu gehören.**

UNSER WICHTIGSTER TIPP: BLEIBEN SIE WACHSAM!

PHISHING-ANGRIFFE
über angebliche Nachrichten Ihrer Sparkasse

Aktuell werden u. a. folgende Phishing-Nachrichten verschickt:

- → **Vorwand einer ablaufenden S-pushTAN-Registrierung**
- → **Vorwand einer Kündigung des Sparkassenkontos**
- → **Vorwand einer Aktualisierung der ID-Check-App**

Über **Links in diesen Nachrichten** landen Sie auf **Phishing-Seiten, die den Sparkassen-Online-Banking-Seiten ähnlich** sind. Dort werden Ihre Online-Banking-Zugangsdaten, weitere persönliche Daten sowie die Nummer Ihrer Sparkassen-Card erfragt.

VORSICHT: GEBEN SIE KEINE DATEN AUF SOLCHEN SEITEN EIN!

Diese könnten von Kriminellen missbraucht werden, um betrügerische Transaktionen durchzuführen oder Sie im Namen der Sparkasse anzurufen.

HÖCHSTE GEFAHR: SMS MIT EINEM pushTAN-REGISTRIERUNGSLINK.

Höchste Gefahr besteht, wenn Sie eine SMS mit einem pushTAN-Registrierungslink erhalten. Bitte **nehmen Sie den Warnhinweis,** der in der SMS enthalten ist, **ernst – leiten Sie den Link nicht weiter –** nicht per SMS, nicht per WhatsApp und kopieren Sie den Link auch nicht auf irgendwelche Internetseiten! Wenn Betrüger die pushTAN übernommen haben, haben sie vollen Zugriff auf Ihr Online-Banking/Ihre Konten.

MICROSOFT-BETRUG

Mehr als 1,4 Milliarden Menschen nutzen Windows 10 und Windows 11. Das ist eine gewaltige Zielgruppe für Kriminelle. Sie versenden **E-Mails mit gefälschten Warnungen** und verweisen auf eine Telefonnummer, die Sie anrufen sollen. Oder es wird durch **Schadsoftware eine Störung auf Ihrem Computer** erzeugt, für deren Behebung Sie eine Telefonnummer anrufen sollen. Dies kann auch durch ein einfaches Pop-up-Fenster geschehen, während Sie im Internet unterwegs sind.

Außerdem rufen **angebliche Microsoft-Mitarbeitende oder angebliche Beschäftigte des Support-Teams von Microsoft** bei Ihnen an. Diese möchten Ihnen beim Beheben eines technischen Problems, beim Schließen einer Sicherheitslücke oder beim Installieren eines wichtigen Updates helfen. **Alles gelogen! Am anderen Ende der Leitung sitzen Kriminelle,** die Ihren Computer kapern wollen. Sie sollen ein Fernwartungstool, eine App oder ein bestimmtes Programm installieren.

Doch wenn Sie dies tun, dann **geben Sie Ihren Computer in fremde Hände!** Wenn Sie aufgefordert werden, eine Supportgebühr zu überweisen oder eine Test-Überweisung vorzunehmen, Online-Banking-Zugangsdaten und andere sensible Daten einzugeben, **dann händigen Sie Kriminellen Ihr Vermögen aus!**

WHATSAPP-BETRUG

Mehr als zwei Milliarden Menschen weltweit nutzen den Messenger-Dienst WhatsApp. Auch diese riesige Gruppe ist ein ideales Ziel für kriminelle Aktivitäten.

„Digitaler Enkeltrick“:
Betrüger versuchen, sich als vertraute Personen auszugeben. Sie erhalten eine **SMS oder eine WhatsApp-Nachricht von einer unbekannten Mobilfunknummer.** Darin erklärt eine Person, die ihren Namen nicht nennt, sie habe eine neue Rufnummer und weist darauf hin, dass sie gern per WhatsApp kontaktiert werden kann. Durch **„Hallo Mama“ oder „Hallo Papa“** wird der Eindruck erweckt, die Nachricht käme von Ihrer Tochter oder Ihrem Sohn. In einer Variante dieses Betruges wird auch behauptet, dies sei das Handy einer Freundin oder eines Freundes, weil das eigene Smartphone verloren oder gestohlen worden sei.

Wenn Sie reagieren, werden Sie später **aufgefordert, eine Überweisung zu tätigen.** Die Gründe können vielfältig sein, z. B. um eine dringende Rechnung zu bezahlen, eine Strafe oder einen Schaden zu begleichen, ein neues Handy zu kaufen oder geliehenes Geld zu erstatten. Es kann auch der Hinweis kommen, dass sich die Bankverbindung geändert habe. **Alles gelogen! Fallen Sie nicht darauf herein!**

KLEINANZEIGEN-BETRUG

Auf **kleinanzeigen.de** (früher: ebay-kleinanzeigen.de) **oder** einer **anderen Verkaufsplattform** bieten Sie ein Produkt zum Verkauf an und eine Person bekundet Interesse. Es wird um die **Nutzung von „Sicheres Bezahlen“** gebeten. Anschließend kommt z. B. eine E-Mail oder SMS, dass die Ware bezahlt sei.

Damit die Auszahlung erfolgen könne, wird **auf einen Link verwiesen.** Doch statt auf dem echten, sicheren Portal landen Sie auf einer **gefälschten Webseite,** die dem Kleinanzeigen-Portal täuschend ähnlich sieht. Dort werden Sie **aufgefordert, Online-Banking-Zugangsdaten, Kreditkarten-Daten** oder andere sensible Informationen **einzugeben.** Tatsächlich wird im Hintergrund eine Überweisung oder andere Transaktion ausgelöst, die Sie unwissentlich freigeben – z. B. weil Ihnen suggeriert wird, dass Sie damit den Kaufpreis annehmen oder die Auszahlung des Verkaufspreises auslösen.

SO VERHALTEN SIE SICH RICHTIG:

Misstrauen Sie am Telefon angezeigten Rufnummern.
Technisch lässt sich jede Rufnummer anzeigen
(z. B. auch 110 für die Polizei oder 09181 210-0 für die Sparkasse Neumarkt-Parsberg).

Anrufe/Nachrichten immer kritisch hinterfragen,
egal über welchen Kommunikationskanal. Im Zweifel rufen Sie unter einer Ihnen bekannten Rufnummer zurück (Sparkasse Neumarkt-Parsberg: 09181 210-0).

Transaktionsdaten in Ihrer pushTAN-App oder auf Ihrem chipTAN-Generator immer kontrollieren.
Denn die Freigabe löst eine Transaktion aus, die zu einer unwiderruflichen Belastung Ihres Girokontos führen kann.

Keine Weiterleitung Ihrer pushTAN-Registrierungsdaten!

Aktualisieren Sie immer Ihre Sparkassen- Apps und Software!

Keine Installation von unbekannten Programmen, Apps und Fernwartungstools,
insbesondere dann, wenn Sie dazu von Dritten aufgefordert werden.

Test-Überweisungen gibt es nicht.
Für die Stornierung von Überweisungen ist keine Freigabe in der pushTAN-App notwendig.

WIR HELFEN IHNEN!

Vermuten Sie, dass Sie **auf einen Betrug hereingefallen** sind?

Rufen Sie **schnellstmöglich** die deutschlandweite **Sperrhotline 116 116 an und informieren Sie uns zeitnah** unter **09181 210-0.**

Aktuelle Informationen zu Betrugsmaschen sowie Sicherheitshinweise finden Sie hier:
www.sparkasse-neumarkt.de/sicherheit

Ihre Sparkasse Neumarkt-Parsberg