Betrug erfolgreich verhindern

**Betrüger lauern an allen Ecken, vor allem im Internet.
Die Methoden, mit denen man sich schützen kann sind oft simpel, erfordern jedoch ein wenig Arbeit und Aufmerksamkeit.**

Was kann ich selber für mich tun, um Betrug zu vermeiden?

Verbesserung der IT-Sicherheit zu Hause durch:

- Einsatz eines Virenscanners und einer Firewall selbst kostenlose Software bietet einen guten Schutz – Updates sollten bei jeder PC-Nutzung (optimal wäre automatisch) installiert werden.
- Nutzung von Virenscannern bei mobilen Endgeräten (Tablets & Smartphones)
- Regelmäßige Aktualisierung des Betriebssystems bei allen verwendeten Endgeräten
- Verwendung von sicheren Passwörtern.
  Sie können sich komplexe Passwörter schwer merken. Wie es funktioniert erklärt diese Website:
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
- Wenn Sie eine Aufforderung zur Eingabe einer TAN erhalten, weil Sie sich auf einem neuen (bislang unbenutzten) Gerät anmelden, dann geben Sie diese TAN nur heraus, wenn Sie das Gerät auch wirklich selber aktiviert haben. Betrüger versuchen so, eigene Geräte freizuschalten und Ihr Gerät im Anschluss zu sperren
- Prüfen Sie Ihre Versicherungspolicen, ob Sie gegen Cyber-Risiken (Onlinebanking-betrug, Identitätsdiebstahl etc. versichert sind). Bei der R+V kann man das über die Hausratversicherung sehr günstig mitversichern lassen.

Welche Hilfsmittel bietet Ihnen die Volksbank Heinsberg eG zu Ihrem Schutz?

- Sichere Homepage erkennbar am Kürzel: https://
- Sichere TAN Verfahren (z. B. über die App VR-SecureGo Plus)
- Tageslimite einrichten, minimiert das Restrisiko
- Sicherer Browser: VR-Protect – Dieser wurde nur für die Volksbank Heinsberg programmiert und kann nur für eBanking benutzt werden.
- Sperre von beleghaften Überweisungen, falls Sie ausschließlich eBanking nutzen
- Der VR-Computercheck prüft Ihren Computer, Ihr Tablet und Ihr Smartphone auf Sicherheitslücken
- https://www.volksbank-heinsberg.de/digitales-banking/sicherheit/vr-computercheck.html
- Sperr-App 116 116 falls Karten- oder Online-Daten entwendet wurden

Welche Arten von Betrug gibt es und wie können Sie sich schützen?

Hacking-Angriff auf Ihren Rechner und/oder Onlinebanking

- Firewall installieren und ständig aktualisieren, sichere Passwörter benutzen (siehe Seite 1) und WLAN vor Fremdzugriff schützen.

Phishing per Mail

- Alle Mails genau lesen. Auf korrekte Rechtschreibung und Anrede achten, da Phishingmails oft fehlerhaft sind.
- NIEMALS Links unbekannter Mailabsender anklicken. Die Gefahr, dadurch einen Virus zu laden oder eine gefälschte Internetseite zu besuchen ist sehr hoch.
- NIEMALS vertrauliche Zugangsdaten (PIN/TAN) eingeben, wenn Sie von Mails unbekannter Absender dazu aufgefordert werden.
- Keine Bank wird Sie je per Mail oder Telefon dazu auffordern zwecks Überprüfungen vertrauliche Daten preiszugeben!

Anrufe von angeblichen Firmen, Institutionen oder Bankmitarbeitern

- Oft gibt sich ein Anrufer als Mitarbeiter der Sicherheitsabteilung von z. B. Microsoft aus und behauptet, Sie hätten einen Virus auf dem Rechner und nur er könne ihn beseitigen.
  Wenn das passiert – SOFORT AUFLEGEN!
- Microsoft kennt im Normalfall weder Ihre Telefonnummer noch Ihren Namen.
- Microsoft würde Sie niemals anrufen, weil es keine Möglichkeit gibt, Ihren PC von dort aus zu überwachen.
- Und sollten Sie dennoch mit dem Anrufer sprechen: Geben Sie UNTER KEINEN UMSTÄNDEN vertrauliche Daten (z. B. PIN/TAN) preis, wenn Sie dazu aufgefordert werden.

Warenbetrug (gefälschte oder gehackte Internetshops oder Shops bei Amazon, eBay & Co.)

- Ein paar einfache Regeln helfen dabei so genannte Fakeshops zu erkennen: Informationen dazu erhalten Sie hier: https://www.volksbank-heinsberg.de/fake-shops
- Grundsätzlich gilt: Verzichten Sie auf JEDEN Kauf, gegen Vorkasse per Überweisung, wenn Sie den Empfänger/Shop nicht kennen, da Sie keinerlei Möglichkeiten haben, Ihr Geld im Ernstfall zurückzubekommen.
- Wählen Sie Shops mit sicheren Bezahlmethoden (Kreditkarte, paydirekt, etc.). Hier haben Sie im Bedarfsfall ein Rückerstattungsrecht. Beachten Sie dazu auch den folgenden Punkt:

IBAN des Empfängers unter die Lupe nehmen

- Achten Sie auf die ersten beiden Buchstaben der IBAN. Diese sollten für das Land des Internetshops stehen. Ist der Shop aus Deutschland (www.xxx.de)? Dann sollte die IBAN auch mit DE beginnen.
- Oft befinden sich die Bankverbindungen von betrügerisch verwendeten Internetshops im Ausland (z. B. ES = Spanien, IE = Irland). Das sieht nicht nur unlogisch aus, sondern ist es meistens auch, also besser – FINGER WEG.

Hilfreiche Webseiten:

Die Seite des Bundesamtes für Sicherheit in der Informationstechnik – hier kann man auch kostenlos nützliche Newsletter zur IT-Sicherheit abonnieren:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

Außerdem finden Sie auf unserer Seite viele hilfreiche Tipps:
https://www.volksbank-heinsberg.de/sicherheit-im-netz

Volksbank Heinsberg eG
Persönlich · Fair · Genossenschaftlich