Angst ist ein schlechter Ratgeber, aber Vorsicht die Mutter der Porzellankiste! Aber wer ausreichend informiert ist, wird selten(er) Opfer von Online-Betrügern und ähnlichen Gaunern. Wir möchten Ihnen mit den vorliegenden Infos ein Stück weit jene Sicherheit geben, die nötig ist, um im Internet gut und sicher unterwegs zu sein.

Sicherheit geht vor!

Tipps & Tricks zur Vermeidung von Betrugsfällen u. ä.

Raiffeisenkasse Meran Oktober 2024

Raiffeisen Meran

Phishing

Phishing (vom englischen „fishing“ = Angeln) ist ein Sammelbegriff für Versuche, über **Spam-Mails** oder Direktnachrichten sowie über fingierte Webseiten oder Profile an die **persönlichen Daten** eines fremden Benutzers zu gelangen. Ziel von Phishing sind der Eigentums- und Datenklau, der bis hin zur vollständigen Kontoplünderung oder sogar einem Identitätsdiebstahl führt. Es handelt sich dabei um einen Link der auf eine gefälschte Webseite führt und der darauf abzielt sensible Daten zu erlangen:

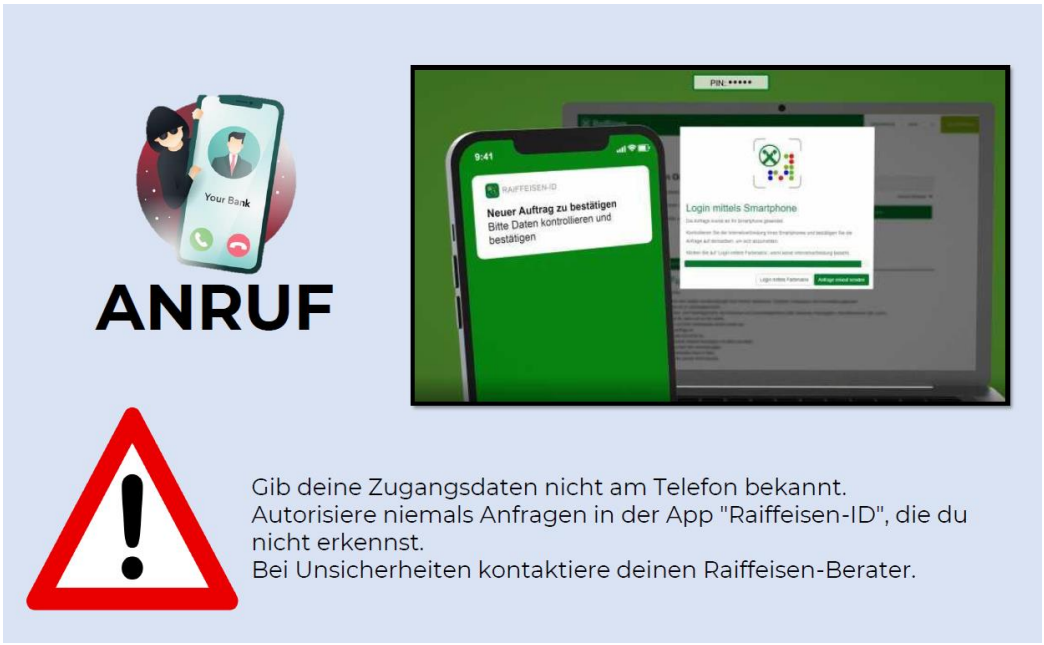
- Kartennummern
- Bankdaten
- Passwörter
- usw.

Smishing

Der Begriff **Smishing** setzt sich aus den Wörtern „**SMS**“ und „**Phishing**“ zusammen und bezeichnet damit **Phishing per SMS**. Die Angreifer versenden dabei Textnachrichten per SMS und fordern den Empfänger darin zu einer dringend notwendigen Handlung auf, die meist über den Klick auf einen **Link** durchzuführen ist.

Vishing

Der Begriff Vishing ist eine Abkürzung für „Phishing via VoIP“ oder „Voice Phishing“ und beschreibt den Datendiebstahl via Telefon. Im Gegensatz zum klassischen Phishing (meist via E-Mail) machen sich Betrüger beim Vishing den Vorteil des „persönlichen Kontakts“ am Telefon zunutze.

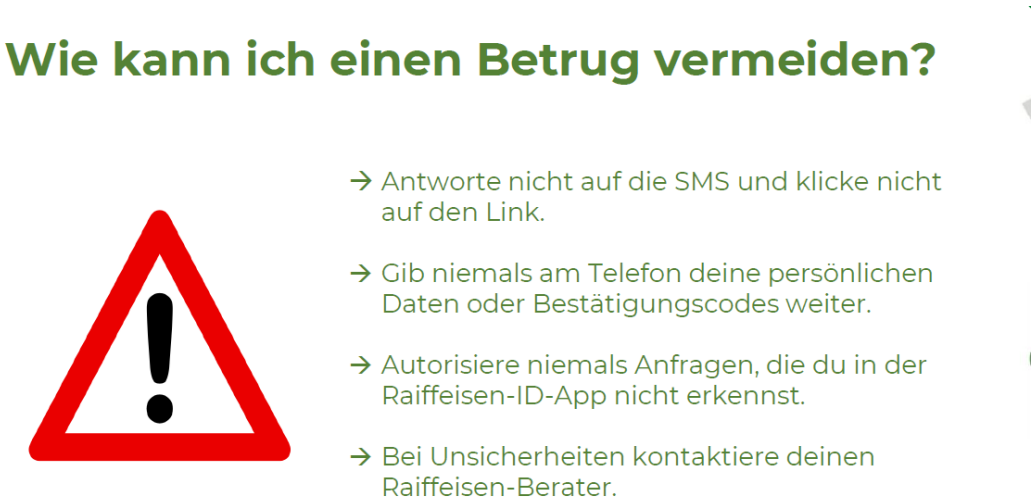


Merkmale einer dieser Betrugsfälle

- Mail enthält Links oder Anlagen
- Dringliche Handlung
- Drohung
- Aufforderungen
- Absender bekannt, Anliegen ungewöhnlich

Tipps wie man sich schützen kann

- Absender kontrollieren (Vorsicht bei neuem oder seltenem Absender)
- Allgemeinen Aufbau der Mail kontrollieren
- Logischen Inhalt der Mail hinterfragen
- Aufforderungen / Dringlichkeiten hinterfragen
- Bei Zweifel / Unsicherheit NIE Links und / oder Anlagen öffnen



Logik hinterfragen

- Mail vom Paketdienst erhalten → Habe ich ein Paket bestellt?
- Mail vom Finanzinstitut mit Aufforderung zur Eingabe von Zugangsdaten, Sicherheits-PIN‘s usw. → KEIN Finanzinstitut fragt nach derartigen Daten
- Mails mit unerwarteten Gewinnen → LÖSCHEN

Link überprüfen

- Mit der Maus über den Link fahren **(nicht Klicken!)**
- Beim Handy → langes drücken auf den Link **(nicht Klicken!)**

Zusammenfassung

Grundsätzlich ist wichtig erhaltene Mails gut zu überprüfen, wenn Links oder Anhänge enthalten sind. Man muss sich der Gefahr von Phishing bewusst sein und diese im Hinterkopf behalten damit man nicht in die Falle tappt.

- **Wachsamkeit** ist der beste Weg, um Phishing-Betrug zu erkennen
- **Merkmale von Phishing-Mails** im Hinterkopf behalten
- **Links überprüfen**

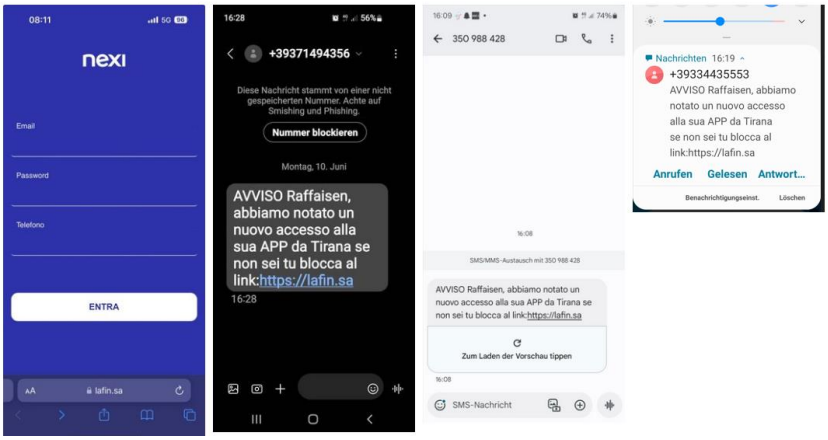
Beispiele für Smishing und Vishing und Phishing in der Raiffeisen Welt

https://www.raiffeisen.it/de/cybersecurity/aktuelle-warnungen.html#c117496

Bei dieser Betrugsmasche erhält der Kunde eine Phishing-SMS, in der er aufgefordert wird, sich über den zugesandten Link bei Nexi anzumelden. Der Link führt zu einer Phishing-Seite, die den Zugang zu Nexi nachbildet und zusätzlich zu Benutzername und Passwort nach der Telefonnummer fragt. In der offiziellen Nexi-App wird die Telefonnummer nie abgefragt. Sobald die Betrüger in den Besitz der persönlichen Daten, wie Benutzername und Telefonnummer, gelangt sind, wird der Kunde darüber informiert, dass betrügerische Überweisungen zu blockieren sind, und aufgefordert, die Transaktionen zu autorisieren, um die Zahlungen zu blockieren. Die erbetenen Genehmigungen zielen jedoch nicht auf die Sperrung von Zahlungen ab, sondern auf die Genehmigung von Sofortüberweisungen zugunsten der Betrüger.

Wie du dich schützen kannst:

Autorisiere niemals Anfragen, die du in der Raiffeisen-ID-App nicht erkennst.



Beispiele für Smishing und Vishing und Phishing in der Raiffeisen Welt

https://www.raiffeisen.it/de/cybersecurity/aktuelle-warnungen.html#c117496

Bei dieser Betrugsmasche erhält der Kunde eine Phishing-SMS, in der er aufgefordert wird, sich über den zugesandten Link bei Nexi anzumelden. Der Link führt zu einer Phishing-Seite, die den Zugang zu Nexi nachbildet und zusätzlich zu Benutzername und Passwort nach der Telefonnummer fragt. In der offiziellen Nexi-App wird die Telefonnummer nie abgefragt. Sobald die Betrüger in den Besitz der persönlichen Daten, wie Benutzername und Telefonnummer, gelangt sind, wird der Kunde darüber informiert, dass betrügerische Überweisungen zu blockieren sind, und aufgefordert, die Transaktionen zu autorisieren, um die Zahlungen zu blockieren. Die erbetenen Genehmigungen zielen jedoch nicht auf die Sperrung von Zahlungen ab, sondern auf die Genehmigung von Sofortüberweisungen zugunsten der Betrüger.

Beispiele für Social Engineering in der Raiffeisen Welt

https://risbz.atlassian.net/wiki/spaces/SD/pages/1801011283/Betrugsf+lle+mit+Social+Engineering#Betrugsf%C3%A4llemitSocialEngineering-GesperrteBanken

Was ist Social Engineering?

Beim *Social Engineering* wird ein Kunde persönlich kontaktiert und beeinflusst. Dabei wird von Seiten des Kunden oder auch durch Bankmitarbeiter vorher Informationen zum Opfer gesammelt. Diese Informationen werden anschließend benutzt, um das Vertrauen des Kunden zu gewinnen. Der Kontakt zu den Kunden kann über SMS, E-Mail und telefonisch erfolgen. Wahrscheinlich ist eine Kombination verschiedener Kontaktwege. Dabei gewinnt der Betrüger telefonisch das Vertrauen des Kunden, indem er gesammelte Informationen einbringt. So kann er Kunden dazu bringen, persönliche Informationen und Zugangsdaten preiszugeben. Außerdem können Kunden sogar angeleitet werden, die betrügerischen Aufträgen in den eigenen Authentifizierungssystemen freizugeben.

Allgemeine Cybersecurity Tipps – Empfehlungen

- **Erstellung von Backups**
- **System aktuell halten – regelmäßige Installation von Updates**
- **Installation von einem Antivirusprogramm**
- **Tipps zu Passwörtern**
  1. Zugangsdaten geheim halten!
  2. Zugangsdaten sicher verwahren!
  3. Ein gutes Passwort wählen!

Ein gutes Passwort…

… nicht von der Person auf das Passwort schließen
… ist niemandem bekannt und wird andernfalls sofort geändert
… ist mindestens 12 Stellen lang
… besteht aus Buchstaben, Zahlen und Sonderzeichen
… hat kein Zeichen, das mehr als zweimal vorkommt
… wird regelmäßig geändert
… wird nicht auf mehreren Systemen oder Anwendungen eingesetzt

(Bsp. Mein Auto steht seit Januar 2017 in der Garage > Mas$J2017idG

Viren - Malware

Ransomware

Ransomware ist eine Form von schädlicher Software (Malware), die darauf abzielt, den Zugriff auf ein Computersystem oder die darin enthaltenen Daten zu blockieren oder zu verschlüsseln. Die Angreifer verlangen dann von den Opfern die Zahlung eines Lösegelds, häufig in Kryptowährung, um den Zugriff auf ihre Daten wiederherzustellen.

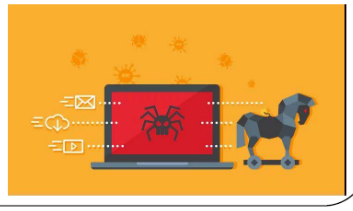
Malware

Worm

Ein Worm (Wurm) ist eine Art schädlicher Software (Malware), die sich selbstständig verbreitet, indem sie Kopien von sich selbst auf andere Computer oder Systeme überträgt. Worms können erheblichen Schaden anrichten, indem sie Netzwerkressourcen beeinträchtigen, Daten zerstören oder verändern sowie die Leistung von Computersystemen beeinträchtigen.

Trojan

Ein Trojaner ist eine Art schädlicher Software, die sich als legitime Anwendung tarnt, um unbemerkt in ein Computersystem einzudringen. Sobald aktiviert, ermöglicht der Trojaner Hackern den Zugriff auf das infizierte System, um Daten zu stehlen, Kontrolle zu übernehmen oder andere schädliche Aktivitäten auszuführen.



Nähe ist Raiffeisen.

Jetzt noch einfacher und schneller deine Bankgeschäfte online erledigen:

- Termine vereinbaren
- Raiffeisen Debit Card bestellen
- Echtzeitüberweisung tätigen
- Karte fürs Ausland freischalten
- Verträge unterschreiben
- Profildaten ändern

www.raiffeisen.it