

Merkblatt Schutz vor Betrug per E-Mail, Telefon, SMS und WhatsApp

Betrugsnachrichten sind leider keine Seltenheit und es werden immer mehr. Auch Mitglieder der Naturfreunde waren in letzter Zeit mehrfach davon betroffen.

Um sich vor Betrugsnachrichten zu schützen, gibt es verschiedene Massnahmen, mit denen das Risiko minimiert werden kann.

Nachfolgend zeigen wir dir, worauf du beim Thema Betrugsnachrichten achten solltest.

Betrugsnachrichten reduzieren

Es gibt zwar Möglichkeiten, die Anzahl der Betrugsnachrichten zu reduzieren, leider lassen sie sicher aber nicht vollständig vermeiden.

Es ist deshalb weiterhin wichtig, vorsichtig zu sein und bei verdächtigen Nachrichten oder Anrufen richtig zu reagieren.

Öffentliche Kontaktdaten

Betrüger suchen im Internet nach öffentlich zugänglichen Kontaktdaten (E-Mail-Adressen und Telefonnummern), welche sie für ihre Betrugsmaschinen kontaktieren können.

Wenn deine E-Mail-Adresse oder Telefonnummer auf der Naturfreunde-Webseite im Bereich «Über uns» immer ersichtlich ist, steigt das Risiko, dass du von Betrügern kontaktiert wirst.

Um das Risiko zu vermeiden, sollten die E-Mail-Adresse und Telefonnummer erst in der Anmeldebestätigung der Aktivität stehen.

Wenn das nicht möglich ist, empfehlen wir dir, deine private E-Mail-Adresse durch eine Naturfreunde-E-Mail-Adresse zu ersetzen. Falls du noch keine Naturfreunde-E-Mail-Adresse hast, können wir dir eine erstellen. Dabei kann auch eine Weiterleitung auf deine private E-Mail-Adresse konfiguriert werden.

Deine private Telefonnummer solltest du von der Naturfreunde Webseite entfernen. Der erste Kontakt sollte dann über die E-Mail-Adresse erfolgen.

Spam-Filter

Spam-Filter können verdächtige Nachrichten und Anrufe aufgrund unterschiedlicher Merkmale automatisch erkennen. Je nach Anwendung werden diese direkt blockiert, als Spam gekennzeichnet oder in einen separaten Ordner verschoben.

E-Mail-Spam-Filter

Ein E-Mail-Spam-Filter kann in den meisten E-Mail-Programmen aktiviert werden. Für Microsoft Outlook gibt es dazu folgende Anleitung: [Outlook Spam-Filter](#)

Wenn du eine Naturfreunde-E-Mail-Adresse verwendest, kannst du unter Umständen auch noch weitere Filter konfigurieren: [Hostpoint Spam-Filter](#)

Telefon-Spam-Filter

Für Anrufe kann ein Spam-Filter in den Einstellungen der meisten modernen Smartphones aktiviert werden. Bei Android-Geräten heisst die entsprechende Einstellung «Anrufer-ID und Spam-Schutz».

Bei Schweizer Telekomprovider können zusätzliche Spam-Filter aktiviert werden. Für Swisscom gibt es folgende Anleitung: [Swisscom Spam-Filter](#)

SMS-Spam-Filter

Für SMS kann ein Spam-Filter in den App-Einstellungen unter «Messages-Einstellungen -> Sicherheit und Datenschutz -> Spamschutz» aktiviert werden.

WhatsApp Spam-Filter

WhatsApp bietet verschiedene Schutzfunktionen gegen unerwünschte Nachrichten. Unter «Einstellungen -> Datenschutz -> Erweitert» kann die Funktion «Nachrichten von unbekannten Konten blockieren» aktiviert werden. Sie blockiert Nachrichten von unbekannten Konten, welche viele Nachrichten versenden.

Betrugsnachrichten erkennen

Betrugsnachrichten sind oft nicht auf den ersten Blick als solche erkennbar. Darum ist es wichtig, sich Zeit dafür zu nehmen und Nachricht gründlich zu prüfen.

Falls du dir bei einer Nachricht nicht sicher bist, ob es sich um einen Betrug handelt, frage lieber bei jemanden um Rat, bevor du darauf reagierst. Vier Augen sehen mehr als zwei!

Unbekannt Telefonnummer

Wenn du eine Nachricht oder einen Anruf von einer dir unbekannten Telefonnummer erhältst, solltest du grundsätzlich immer vorsichtig sein.

Gewöhne dir an, bekannte Telefonnummern abzuspeichern und Telefonnummern, von denen du Spam-Nachrichten erhältst, zu blockieren.

Absender-E-Mail-Adresse

Die Betrugsmasche funktioniert, indem du eine E-Mail von einer möglichst vertrauenswürdig wirkenden Adresse erhältst. Wenn nur ein einzelner Buchstabe geändert wird, ist dies kaum zu erkennen und ist trotzdem eine andere E-Mail-Adresse.

Zum Beispiel sind folgende zwei E-Mail-Adressen unterschiedlich (bei einer Adresse wurde das kleine «l» zu einem grossen «I» geändert):

- heinz.vogt@naturfreunde-kloten.ch
- heinz.vogt@naturfreunde-kloten.ch

Schreibfehler & Stil

Solche Betrugsmaschen funktionieren in der Regel eher über Quantität als über Qualität und weisen oft ähnliche Merkmale auf:

- Schreibfehler
- Ungebräuchliche Schreibweisen (ß anstatt ss)
- Es ist dringend
- Es kann nicht telefoniert werden
- Es geht um Geld

Richtig reagieren, wenn man eine Betrugsnachricht erhält

Eine Betrugsnachricht ist an sich nicht automatisch gefährlich. Betrüger versuchen über den Kontakt jedoch häufig, dich dazu zu bringen, persönliche Informationen weiterzugeben, Geld zu überweisen oder schädliche Dateien zu öffnen.

Wenn du vermutest, eine Nachricht ist verdächtig:

- Antwort nicht auf die Nachricht
- Klick auf keine Links
- Öffne keine Dateien
- Überweise kein Geld

Richtig reagieren, wenn man es zu spät erkannt hat

Auch wenn man vorsichtig ist, kann es trotzdem passieren, dass man ein Betrug zu spät erkennt. Wichtig ist dann, möglichst schnell zu handeln, um den Schaden zu minimieren.

Welche Schritte dafür notwendig sind, hängt davon ab, was genau passiert ist.

- Passwort eingegeben -> Passwort ändern
- Kreditkartendaten angegeben -> Karte sperren
- Geld überwiesen -> Bank informieren
- Datei geöffnet -> Gerät auf Schadsoftware prüfen

Bei Fragen oder Unsicherheiten kannst du dich jederzeit an
support@naturfreunde.ch wenden.