kabelplus

Pixabay.com cc0

Digitale Treffpunkte
Aktuelles zum Internetbetrug

Hannes Giefing

kabelplus

Das erwartet Sie heute:

Themen

- Ping Calls
- Microsoft Anrufe
- Verdächtige SMS
- Erpresser E-Mails
- Tipps und Tricks

Pixabay.com cc0

kabelplus

Ping Calls

- Lockanrufe
- unbekannte, meist ausländische Nummern +222, +257, +216
- Mehrwertnummern
- beim Annehmen oder Rückruf oft unverständliche Tonbandansagen

Pixabay.com cc0

kabelplus

Ziel von Ping Calls

- Gespräch so lange wie möglich aufrecht erhalten
- Kriminelle Anrufende verdienen an den kostspieligen Mehrwertnummer
- mindestens € 3,-- pro Minute
- keine Grenzen nach oben

Pixabay.com cc0

kabelplus

Wie kommen Kriminelle an Ihre Telefonnummer?

- Telefonbücher
- öffentliche Register/Datenbanken
- oft automatisch generiert
- wahllose Anrufe
- Vorsicht bei der Angabe von Telefonnummern bei unseriösen Online-Shops

Pixabay.com cc0

kabelplus

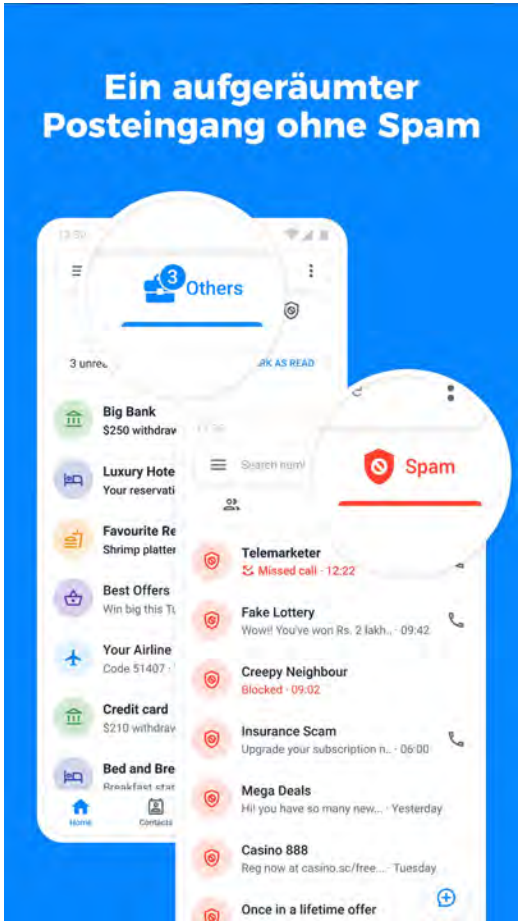
Schutz vor Ping Calls

- kein Annehmen und Rückrufen von unbekannten „ausländischen“ Telefonnummern
- unbekannte Nummer „googeln“
- Telefonnummer blockieren
- App “Truecaller“ installieren

Pixabay.com cc0

kabelplus

Truecaller App für Android und iOS



play.google.com/

kabelplus

Truecaller App für Android und iOS

- Anrufer-ID identifiziert jeden, der Sie anruft
- Automatische Identifizierung unbekannter SMS
- Automatisches Blockieren von Spam und Telemarketing-SMS
- Anzeigen von Namen unbekannter Nummern in der Anrufliste
- Spam und Telefonverkäufer blockieren

play.google.com/

kabelplus

Microsoft-Anrufe

- Kriminelle geben sich als Microsoft Mitarbeiter*innen aus
- Achtung „Betrugsmasche“
- Der Fachbegriff dazu lautet „Tech-Support-Scam“

Microsoft

Pixabay.com cc0

kabelplus

Wie genau funktioniert diese Betrugsmasche?

- Das Telefon läutet und der Anrufer/ Anruferin stellt sich als Microsoft Mitarbeiter*in vor
- Die Anruferin oder der Anrufer erklärt meistens in schlechtem Deutsch, dass der Computer mit Virus infiziert wurde.
- Oder es gibt ein anderes Problem (z.B. fehlerhaftes Update.

Microsoft

Pixabay.com cc0

Wie genau funktioniert diese Betrugsmasche?

- Es wird angeboten, dass Problem gemeinsam zu lösen.
- Dazu sollen Sie ein Fernwartungsprogramm installieren, damit der Fake-Mitarbeitende auf Ihren Computer zugreifen kann.
- Sobald Sie die Software installiert haben, können Betrügende auf Ihren Computer zugreifen und Daten ausspionieren.
- Statt Anrufen werden aber auch Pop-Ups bzw. E-Mail dazu missbraucht.

Microsoft

Pixabay.com cc0

kabelplus

Wie schütze ich mich davor?

- Sofort auflegen falls Microsoft anruft.
- Nicht auf E-Mails oder Pop-Ups reagieren.
- Installieren Sie keine „Ferwartungssoftware“ oder unbekannte Programme.
- Lassen Sie sich nicht durch Drohungen einschüchtern.
- Oftmals drohen Kriminelle damit das Betriebssystem zu löschen, falls Sie den Anweisungen nicht Folge leisten.

Microsoft

Pixabay.com cc0

kabelplus

Was kann ich tun, wenn schon etwas passiert ist?

- Entfernen von unerwünschten Programmen (IT-Fachpersonal).
- Bei Bekanntgabe von Bankdaten unverzüglich Ihre Bank kontaktieren.
- Ändern Sie unverzüglich Ihre Passwörter bei Benutzerkonten, wo Sie sich während des Betruges eingeloggt haben.
- Erstatten Sie Anzeige bei der Polizei.

Microsoft

Pixabay.com cc0

Was kann ich tun, wenn schon etwas passiert ist?

Melden Sie den Betrug an Microsoft!

https://www.microsoft.com/de-DE/concern/scam

kabelplus

SMS-Betrug

Sie haben 1 neue Voicemail. Gehen Sie zu http://ragazzabela.com/vm/?056gdaibi

Sie haben ein ausstehendes Bußgeld, vermeiden Sie rechtliche Schritte, indem Sie die Zahlung sofort hier vornehmen: https://lpdgeldstrafe.me/zahlung.php

Jemand {gj} hat Ihre Bilder (myv) hochgeladen.
Ein ganzes [0v] Album ist hier hochgeladen: https://www.citropicol.com/v/?3hch91erbi [o] c4zyqm

Ihre Sendung geht soeben in Zustellung, verfolgen Sie Ihre Sendung unter https://www.reveusechronique.ch/click.php?o5z548ory k62ibc

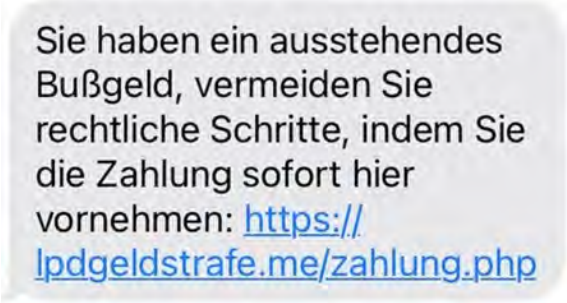
NACHRICHTEN Vor 4 Min.
+43 676 3857920
Ihre Sendung geht soeben in Zustellung, verfolgen Sie Ihre Sendung unter https://t-hacks.net/click.php...

Wir konnten heute ein Paket nicht zustellen. Bitte besuchen Sie: http://oexcelence.com/i.php?b6pcrj9y1j h79j9mk

kabelplus

SMS Betrug - Landespolizeidirektion

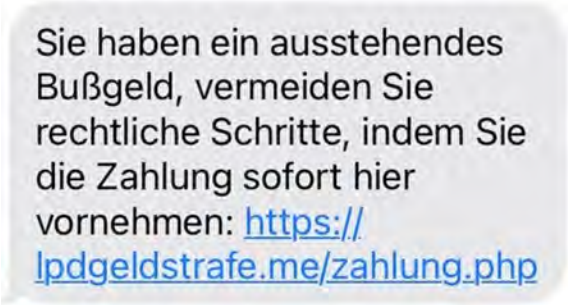
- Die Empfänger*innen werden aufgefordert einen Link aufzurufen um die Bußgeldzahlung durchführen zu können.
- Man kann aber auch aufgefordert werden eine bestimmte App zu installieren.



kabelplus

Was passiert wenn ich den Link öffne?

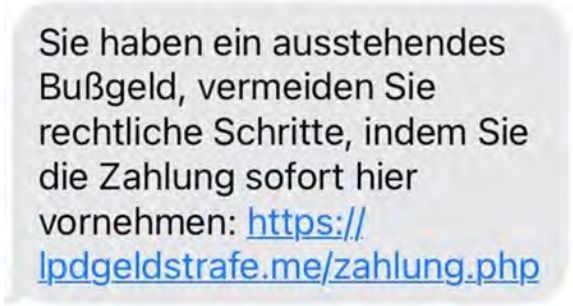
- Es werden Zahlungen per Kreditkarte verlangt um in Abo-Fallen gelockt zu werden.
- Man wird dazu verleitet Apps zu installieren, die Schadsoftware enthalten.
- Diese Schadsoftware kann dann Daten ausspionieren oder auch zu technischen Problemen führen.



kabelplus

Wie schütze ich mich davor?

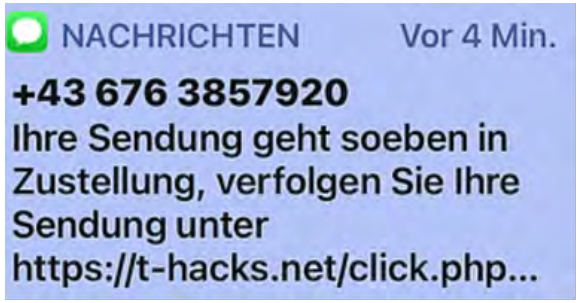
- Nicht auf die SMS reagieren und sofort löschen.
- Den Link in der SMS nicht öffnen.
- Keine Apps installieren.
- Bei Fragen die zuständige Polizeiinspektion kontaktieren.



kabelplus

SMS Betrug – gefälschte Sendungsverfolgung

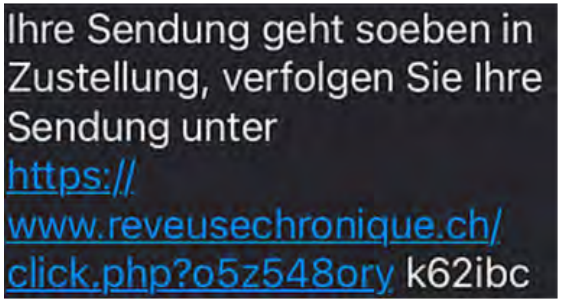
- Betrüger*innen versenden SMS mit gefälschten Paketinformationen zu einer Bestellung.
- Die SMS enthält Nachrichten wie „**Paket konnte nicht zugestellt werden“** oder **“Sendungsverfolgung ist jetzt möglich“.**
- Man wird aufgefordert einen Link zu öffnen.



kabelplus

Wie kann ich Fake-SMS von echten SMS unterscheiden?

- Die SMS enthält einen seltsamen Link.
- Die SMS enthält viele Fehler.
- Überlegen Sie, ob Sie ein Paket erwarten.
- Viele Paketdienstleister versenden Informationen nicht per SMS.
- Achtung auch vor gefälschten E-Mails.

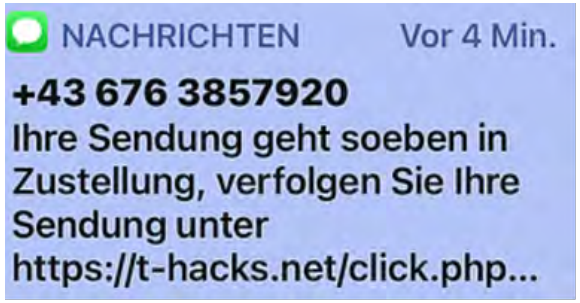


kabelplus

Was passiert wenn ich den Link öffne?

Datendiebstahl

- Sie werden auf eine gefälschte Seite des Paketlieferdienstes .
- Hier sollen Sie dann persönliche Daten bzw. Kreditkartendaten angeben.

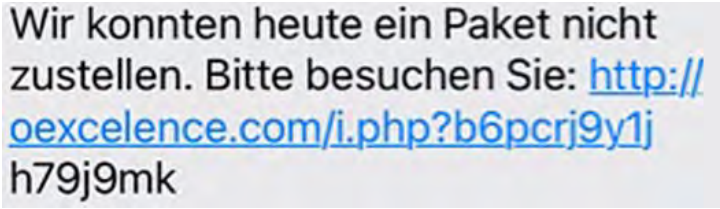


kabelplus

Was passiert wenn ich den Link öffne?

Schadsoftware

- Sie werden auf eine gefälschte Seite des Paketlieferdienstes weitergeleitet.
- Sie werden aufgefordert eine App zu installieren.
- Dadurch kann Schaftsoftware auf Ihren Smartphone installiert werden.
- Damit können z.B. Passwörter ausgelesen werden.

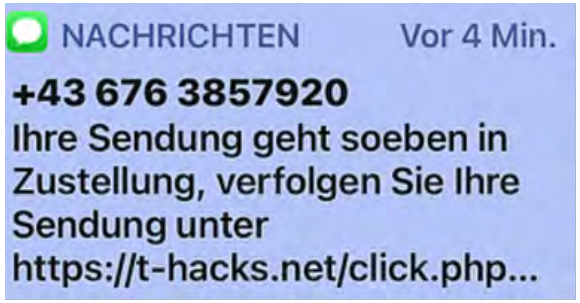


kabelplus

Was passiert wenn ich den Link öffne?

Gewinnspiel

- Der Link in der SMS führt zu einem "FAKE" Gewinnspiel.
- Sie werden aufgefordert Ihre Kreditkartendaten anzugeben.
- Dadurch kann Schaftsoftware auf Ihren Smartphone installiert werden.
- Damit können z.B. Passwörter ausgelesen werden.

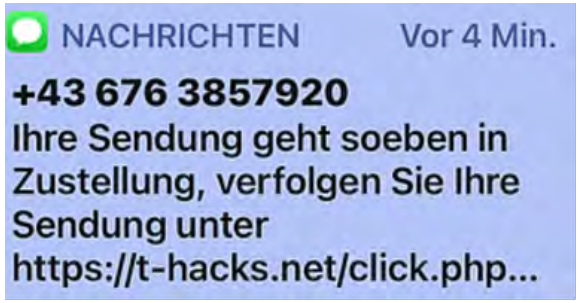


kabelplus

Was passiert wenn ich den Link öffne?

Abofalle

- Sie werden auf eine gefälschte Website des Paketlieferdienstes weitergeleitet.
- Dann werden Sie aufgefordert 1- 2 Euro Versandkosten mittels Kreditkarte zu bezahlen.
- Damit werden Sie in eine Abofalle gelockt.
- Kontaktieren Sie Ihr Kreditkarteninstitut und lassen Sie sofort Ihre Kreditkarte sperren.



kabelplus

Empfang von Betrugs-SMS verhindern?

Sie haben nur die Möglichkeit die Telefonnummer zu blockieren und die Nachricht zu löschen

Android

- Tippen Sie in der Unterhaltung auf die 3 Punkte.
- Wählen Sie anschließend „Nummer blockieren“.

iOS

- Tippen Sie bei der Telefonnummer auf „Info“.
- Wählen Sie anschließend „Anrufer blockieren“.

Pixabay.com cc0

Weitere Beispiele

Kleinanzeigenbetrug mit gefälschter Post-Website

Themen: Geldtransfer, Deals, Soziale Netzwerke, Bank, Kleinanzeigen-Betrug, Phishing

Kriminelle verwenden eine gefälschte Post-Website www.post-service.online für Kleinanzeigenbetrug. Sie suchen nach hochpreisigen Angeboten und geben vor, den Kauf über einen erfundenen Kurierservice der Post abwickeln zu wollen. Ziel ist es, den Opfern das Geld aus der Tasche zu ziehen, denn in weiterer Folge werden Kreditkartendaten abgefragt und die Freigabe einer Zahlung verlangt.

watchlist-internet.at

Weitere Beispiele

Vorsicht, wenn die Wohnungsbesichtigung über booking.com abgewickelt werden sollte

Themen: Geldtransfer, E-Mail, Immobilien, Scamming

Sie haben endlich Ihre Traumwohnung gefunden? Der einzige Haken: Sie sollten schon vor der Besichtigung eine Kaution bezahlen, die angeblich von booking.com verwaltet wird? Dann sind Sie auf ein betrügerisches Wohnungsinserat gestoßen. Zahlen Sie keinesfalls eine Kaution vor der Besichtigung. Diese Wohnung gibt es nicht und Sie verlieren Ihre geleistete Zahlung!

watchlist-internet.at

Weitere Beispiele

Bei diesen Investitionsplattformen verlieren Sie Ihr Geld

Themen: Geldtransfer, Werbung, Soziale Netzwerke, Vorschussbetrug, Scamming, Sonstiges

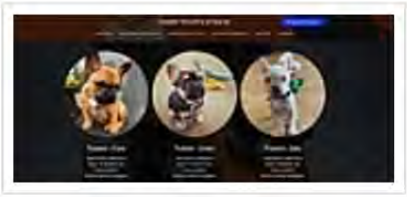
Im Internet findet man unzählige Möglichkeiten, Geld einfach und unkompliziert zu investieren. Auf Trading-Plattformen wie infinitycapitalg.com, suntonfx.com oder windsorglobalaustria.com werden hohe Gewinnchancen, auch ohne großes Finanzwissen versprochen. Klingt zwar sehr verlockend, führt in Wahrheit aber zu sehr hohen Verlusten! Unser Tipp: Checken Sie die Investorenwarnungen der Finanzmarktaufsicht.

watchlist-internet.at

Weitere Beispiele

Vorsicht beim Welpen-Kauf im Internet!

Themen: Online-Shopping, Tiere, Fake-Shops, Sonstiges



Wollen Sie online einen Hundewelpen kaufen? Wenn ja, dann stoßen Sie möglicherweise auf unseriöse Angebote. Der Watchlist Internet werden derzeit zahlreiche Seiten gemeldet, die angeben Rasse-Hundewelpen zu verkaufen und das meist zu einem günstigen Preis. Nicht nur die Preise, sondern auch liebevolle Fotos und Beschreibungen verlocken dazu, einen Kauf zu tätigen. Doch hier gilt es vorsichtig zu sein: Webseiten wie jasminwelpenzuhause.com oder goldenretrieverkonig.de sind unseriös und halten sich nicht an das Tierschutzgesetz!

watchlist-internet.at

Weitere Beispiele

Vorsicht vor unseriösen Shops auf Pinterest

Themen: Online-Shopping, China, Werbung, Deals, Soziale Netzwerke, Markenware, Mode, Fake-Shops, Markenfälschungen

Günstige Modeangebote auf Pinterest entpuppen sich im Nachhinein als Kostenfalle. Oft kommt es zu hohen Lieferkosten, Zollkosten oder Rücksendekosten – Falls Retouren überhaupt akzeptiert werden.

weiterlesen

watchlist-internet.at

kabelplus - Vetriebsmitarbeiter

Für Fragen und Anregungen zu kabelplus Produkten, können Sie sich gerne an unsere Vertriebsmitarbeiter wenden.

Christian Hadl
Region: Mittel- und Südburgenland
Festnetz: 05 0514 13843
Mobil: 0676 810 33843
E-Mail: christian.hadl@kabelplus.co.at

Wolfgang Payer
Region: Nordburgenland
Festnetz: 05 0514 13847
Mobil: 0676 810 33847
E-Mail: wolfgang.payer@kabelplus.co.at