

Zusammenstellung der Qishing-Maschen

Gefälschte Postbriefe: Als neue Masche verschicken Cyberkriminelle perfekt nachgemachte Postbriefe, die angeblich vom Bundesverband deutscher Banken oder von der Finanzgruppe deutscher Sparkassen stammen. Viele Kunden halten diese von der Deutschen Post verschickten Briefe für vertrauenswürdig und scannen den mitgeschickten QR-Code.

Gefälschte Strafzettel: Vor allem Falschparker bekommen hinter die Scheibenwischer geklemmte, täuschend echt aussehende Strafzettel. Für die Bezahlung soll man bloß den falschen QR-Codes einscannen und die dortigen Anweisungen befolgen.

Überklebte QR-Codes: Bei Parkautomaten und Elektro-Ladesäulen wurden echte QR-Codes mit gefälschten geschickt überklebt. Besonders perfide ist die Masche, bei der nach dem Eintippen der Bezahl Daten eine Störung gemeldet wird. Erst im zweiten Anlauf gelangen die Opfer zur richtigen Webseite des Betreibers und vergessen den ersten Fehlversuch.

Manipulierte Rechnungen: In Papierdokumenten und vor allem in Speisekarten und Rechnungen können **Hacker** gefälschte QR-Codes verstecken. Das Bezahlen soll nur über diese QR-Codes möglich sein. Nicht nur im Urlaub werden dabei stark überhöhte Kosten von den Bankkonten der Betroffenen abgezogen.

Gefälschte SMS und WhatsApp-Nachrichten: Immer häufiger verschicken Betrüger gefälschte QR-Codes per SMS oder WhatsApp. Diese Mitteilungen stammen angeblich von bekannten Unternehmen oder von öffentlichen Stellen. Dort wird behauptet, dass die Empfänger noch ihre Schulden bezahlen und dazu den QR-Code nutzen müssten.

Gefälschte E-Mails: Bei dieser schon länger verbreiteten Masche des **Betrugs** erhalten die Opfer eine E-Mail, die vermeintlich von Banken oder beliebten Unternehmen versandt wurde. Das Scannen der enthaltenen QR-Codes und das Eintippen persönlicher Daten sollen die vorgetäuschten Probleme lösen.

Neue Masche - Cybertrading-Betrug

Telefonbetrug:

Update vom 19. März: Kriminelle haben einen Mann im Sauerland um weit mehr als 100.000 Euro gebracht. Dabei gingen die Verbrecher besonders perfide vor:

Sie warnten selbst vor dem Betrugsversuch.

Die Betrüger schickten ihrem Opfer zunächst eine E-Mail, die wie eine Datenabfrage der Industrie- und Handelskammer (IHK) aussah. **Der Mann trug daraufhin persönliche Daten in ein Formular ein.** Am nächsten Tag rief ihn eine angebliche Beraterin seiner Bank an und wies ihn darauf hin, **dass er auf eine betrügerische Mail der IHK hereingefallen und sein Bankkonto gehackt worden sei.**

(Achtung: Eine Bank ruft sie niemals an!!)

Der Mann war misstrauisch - doch die Telefonnummer im Display war offenbar sogar die seiner Bank. Im Glauben, so sein Geld schützen zu können, nannte er bereitwillig wichtige Zugangsdaten zu seinem Konto. Die Kriminellen nutzten diese dann, um mehr als 100.000 Euro auf ihre eigenen Konten zu überweisen.

Wie kann man sich vor dieser Art Betrug schützen? **Bankdaten niemals an Fremde heraus-geben.** Auch die vermeintliche Telefonnummer eines Anrufers ist gefälscht. Beim kleinsten Verdacht solle man lieber schnell **auflegen, Nummer kontaktieren und die Bank selbst unter der bekannten Nummer Kontaktieren**

Vorsicht vor falschen Amazon-Mails:

„Amazon“ behauptet, dass die letzte Zahlungsmethode nicht belastet werden konnte. Die Empfänger werden aufgefordert, ihre Zahlungs-informationen innerhalb von 48 Stunden zu aktualisieren, um eine dauerhafte Kontoschließung zu vermeiden. Laut einer Analyse sind etwa 82 Prozent dieser Fake-Mails inzwischen **KI-gestützt**. Deshalb Vorsicht!!

Außerdem: Links, die direkt in der E-Mail enthalten sind, führen nicht zur echten Amazon-Seite, sondern zu gefälschten Webseiten, die darauf abzielen, persönliche Daten zu stehlen.

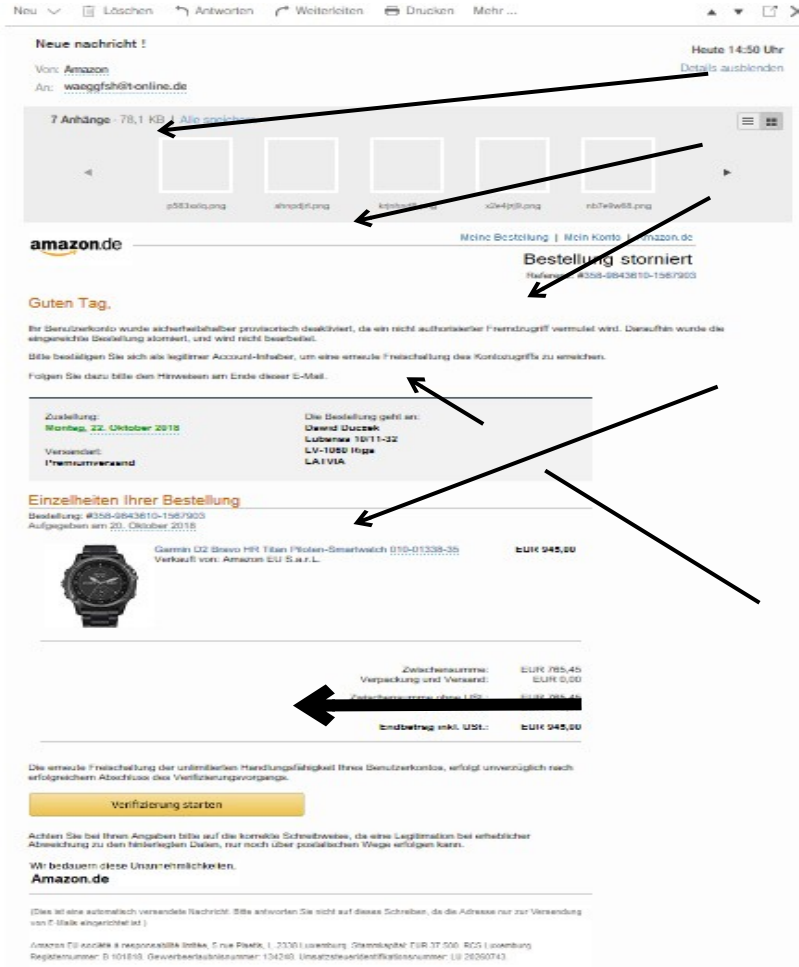
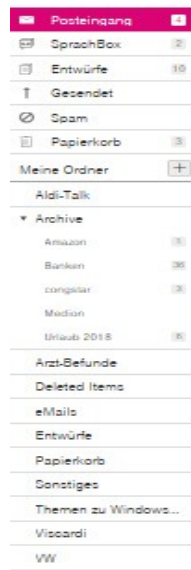
Die **kurzen** Zahlungsfristen setzen den Empfänger unter Druck und können dazu führen, dass er unbedacht handelt. Die Verbraucherzentrale rät dringend davon ab, auf solche E-Mails zu reagieren. Stattdessen sollten sie umgehend in den Spam-Ordner verschoben werden.

Um sicherzugehen, dass keine echte Aufforderung übersehen wird, empfehlen die Verbraucherschützer, direkt auf **der offiziellen Website** oder in der Amazon-App nach ähnlichen Benachrichtigungen zu suchen.

Nebulöse „Rechnungen“

- Scheuen Sie sich nicht eine Kopie der Rechnung an das Unternehmen, von dem diese Rechnung augenscheinlich stammt, zur Überprüfung zu senden. Dies sind speziell **AMAZON** und **Pay-pal**.
- **Ansonsten gleich in den Papierkorb**

Falsche Rechnung von „Amazon“



1) Adresse gekidnappt

2) 5+3 Pings **aktiv**

3) Meine Bestellung, mein Konto **inaktiv**

4) Besteller (nicht ich):

Dawid Duczek

Lubanas 10/11-32

LV-1060 Riga

LATVIA (Lettland)

„Ihr Benutzerkonto wurde sicherheitshalber provisorisch deaktiviert, da ein nicht autorisierter Fremdzugriff vermutet wird. Daraufhin wurde die eingereichte Bestellung storniert, und wird nicht bearbeitet. Bitte bestätigen Sie sich als legitimer Account-Inhaber, um eine erneute Freischaltung des Kontozugriffs zu erreichen.“

Vorsicht!! Text von „Amazon“ ist Fake und soll Sie in Sicherheit wiegen, deshalb ganz schnell „verifizieren“ - nein, nein nein

Hier ist die Falle: Niemals Ihre echten Daten eintragen

MELDUNG AN AMAZON

Sie haben eine eigentümliche Rechnung erhalten. Wenn Sie sich nicht im Klaren sind, so leiten Sie diese einfach weiter an Amazon. In wenigen Minuten erhalten Sie u.U. folgende Nachricht:

Guten Tag Herr 

vielen Dank für das freundliche Telefonat.

Wie besprochen stammt die E-Mail, die Sie erhalten haben, tatsächlich nicht von Amazon.de. Wir sind aber bereits dabei, der Angelegenheit genauer nachzugehen. Wenn möglich schicken Sie uns diese E-Mail als Anhang an: stop-spoofing@amazon.com. So bleiben alle Informationen der Kopfzeile erhalten, mit deren Hilfe wir die Herkunft der E-Mail besser nachverfolgen können. Löschen Sie danach die E-Mail. Wenn Sie die E-Mail nicht als Anhang verschicken können, leiten Sie sie bitte an stop-spoofing@amazon.com weiter. Geben Sie dazu die Information in der Kopfzeile an, wenn dies möglich ist.

Bitte beachten Sie, dass die E-Mail-Adresse stop-spoofing@amazon.com von unserer ameri-kanischen Website Amazon.com betreut wird und Sie daher eine Empfangsbestätigung auf Englisch erhalten werden. Wenn Sie die Mail weder als Anhang senden noch diese weiterleiten können, kann es sein, dass Ihr E-Mail-Provider das Weiterleiten einer bereits erkannten Phishing-Mail blockiert. In die-sem Fall möchten wir Sie bitten, keine Links oder Anhänge zu öffnen und die E-Mail einfach zu löschen

Sie erhalten wichtige Informationen des Kundenservice wie Aktualisierungen der Kontorichtlinien oder Produktrückrufe auch über das Message Center. Sie können das Message Center auch direkt über folgenden Link aufrufen:

<https://www.amazon.de/gp/message>

Lidl-Betrug

Lidl wurde gehackt. Alle Personen, die mit Lidl-Pay einkaufen, wurden von der Fa. Lidl über Datenklau der hier registrierten Kunden gewarnt. Nunmehr erscheint eine neue Masche, mit dem Angebot als treuer Kunde ein Lebensmittelpaket im Gesamtwert von 49,99 € gegen einen kleinen Unkostenbeitrag von 2,99 € als Geschenk zu erhalten. Das ist so geschickt aufgebaut, dass man darauf hereinfällt. In dem Formular werden Bankdaten Ihrer MasterCard mittels „**Umfrage starten**“ abgefragt. **Vorsicht!!**

6054386936@cch1wmacvd.live.nl eine Lebensmittelkiste wert ID520458



Michael von Lidl

Heute, 17:31 Uhr

An: waeggfsh@t-online.de

LIDL Lidl lohnt sich.

Sichern Sie sich Ihre
Lidl Lebensmittelkiste
Über **25.000 €** in kostenlosen
Lebensmitteln - jetzt für Sie!

GRATIS
für Sie bereitgestellt!

Liebe Lidl-Kundin, lieber Lidl-Kunde,
wir möchten Ihnen die einmalige Möglichkeit bieten,
eine Lidl Lebensmittelkiste (im Wert von 49,99 €)
kostenlos zu erhalten. Sie zahlen nur eine geringe
Versandgebühr.

Um sie zu beanspruchen, nehmen Sie einfach an
dieser kurzen **1-minütigen** Umfrage zu Ihren
Einkaufsgewohnheiten und Erfahrungen bei uns teil.

Ihre Meinung zählt!

- Vielfältige Produktauswahl**
Von frischen Lebensmitteln bis zu beliebten Marken
- Hohe Qualität zum kleinen Preis**
Täglich frisch, immer günstig
- Nachhaltig & regional**
Für eine bessere Zukunft
- Kundenzufriedenheit steht bei uns an erster Stelle**
Ihre Meinung hilft uns, noch besser zu werden

UMFRAGE STARTEN →

Datenschutzbestimmungen
Ihre Daten sind bei uns sicher. Das Teilnahmekriterium ist freiwillig.

Nutzungsbedingungen
Nur als Aktionsgeschenk pro Haushalt. Das Angebot gilt nur für begrenzte Zeit.

Hilfereich
Bei Fragen stehen wir Ihnen jederzeit zur Verfügung.

© 2026 Lidl Digital Deutschland GmbH & Co. KG. Alle Rechte vorbehalten.

Lidl - Mehr für Sie.