POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Betrug im Netz

Phishing, Identitätsdiebstahl & Co

Bürgerbefragung zur Cyber-Sicherheit

Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Polizeilichen Kriminalprävention (ProPK),

Jede/r Zehnte gab an, im vergangenen Jahr selbst von Cyberkriminalität betroffen gewesen zu sein.

Am häufigsten wurden Betroffene Opfer von Betrug beim Online-Shopping (23%), Fremdzugriffen auf einen Online-Account, Phishing sowie Betrug beim Online-Banking oder Missbrauch der Kontodaten (je 15%).

Bild: Adobe Stock Polizei NRW

Sich schützen

T k a

Traue keinem anderen

Sich schützen

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Initiative
Sicher handeln

Die SHS-Regel im Überblick

Stoppen

Halte inne. Seriöse Anbieter werden dich nicht zu einer Handlung drängen. Es ist okay, eine verdächtige Anfrage abzulehnen oder zu ignorieren. Wäge stets mögliche Risiken ab – vertraue auf dein Bauchgefühl. Gib grundsätzlich nur zwingend erforderliche Daten preis!

Hinterfragen

Niemand hat etwas zu verschenken. Frage dich: Wie würdest du anstelle deines Gegenübers handeln? Lasse dich nicht von Legenden blenden: Wenn etwas zu gut scheint, um wahr zu sein – ist es nicht wahr! Wenn du dir unsicher bist oder etwas zum ersten Mal tust – informiere dich! Hole dir Unterstützung bei erfahrenen Bekannten oder Experten!

Schützen

Du vermutest einen Betrugsversuch? Schütze dich und andere, indem du Verdächtiges an die jeweilige Plattform meldest. Erstatte gegebenenfalls auch Anzeige bei der Polizei.

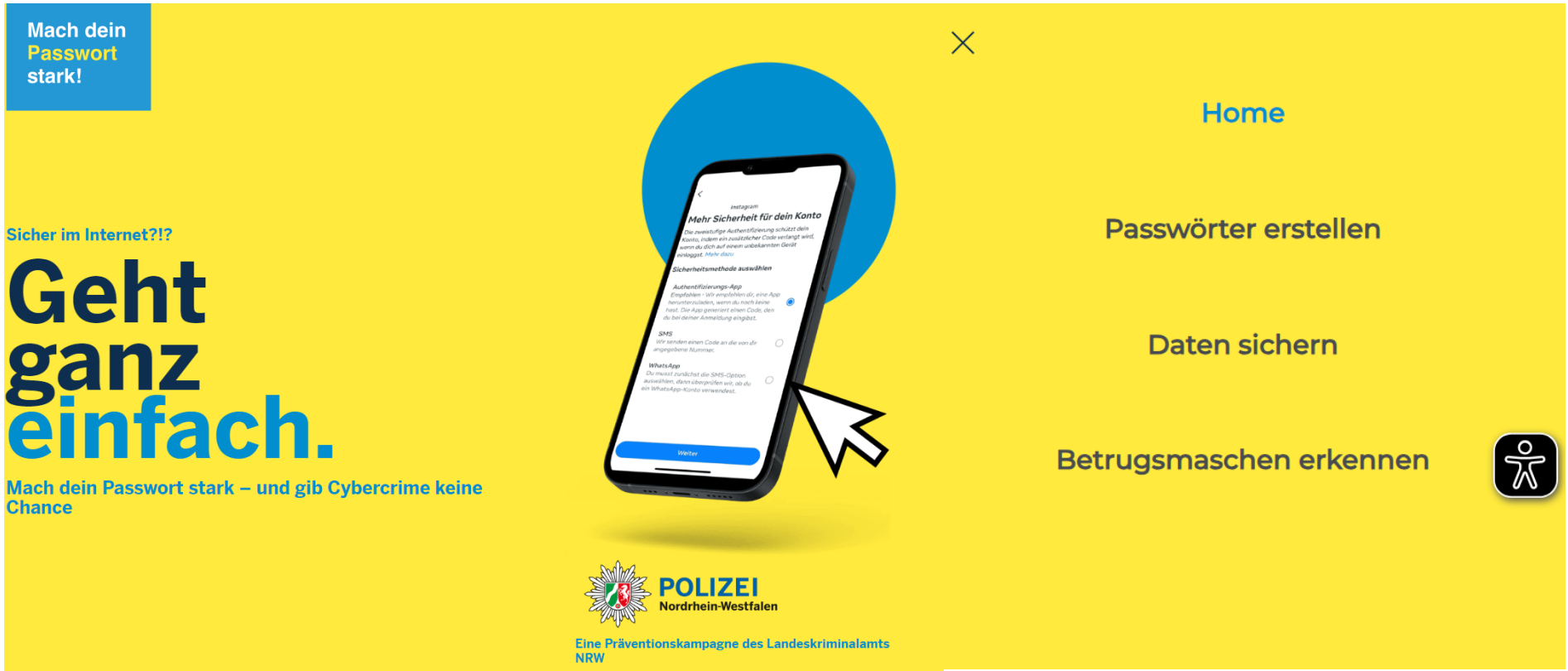
https://www.polizei-beratung.de/themen-und-tipps/sicher-handeln/

Was sind die Gründe dafür, dass Sie nicht alle Schutzmaßnahmen nutzen?

- Ich fühle mich sicher
- Es ist zu kompliziert
- Ich fühle mich überfordert

Sich schützen

https://www.mach-dein-passwort-stark.de



17.03.2025 | Broschüre

Nie zu alt fürs Internet!

Bestellen

Herunterladen (PDF: 5,7 MB)

Ob Kontakt zu Familie und Freunden, aktuelle Informationen oder praktische Helfer für den Alltag – die digitale Welt hat viel zu bieten. Diese Broschüre zeigt älteren Offlinerinnen und Anfängern im Internet, wie sie sicher und selbstbestimmt die ersten Schritte mit Smartphone, Tablet oder Computer wagen. Zudem enthält die Broschüre eine Übersicht mit Anlaufstellen, die persönliche Unterstützung für den Einstieg und das Weiterlernen anbieten.

Recovery-Scam

Kommunikation

E-Commerce

Phising

Dreiecksbetrug

Privat

Networking

Mein digitales Ich

Social Media

Ich habe doch nichts zu verbergen….

Geschäftlich

Love-Scamming

Darstellung

Pig-Butchering

Online-Banking

Betrug mit Online-Geldanlage „Cybertrading Fraud“

E-Government

Quishing

Identitätsdiebstahl

Bild: Adobe Stock Polizei NRW

Moderne Betrugsmaschen

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Quishing

Falsche QR-Codes – Online und Analog

- Bank-Briefe
- Ladesäulen und Parkautomaten
- Plakate im ÖPNV

Bild: Adobe Stock Polizei NRW

https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/quishing-falsche-qrcodes-in-bankbriefen-und-im-strassenverkehr-98612

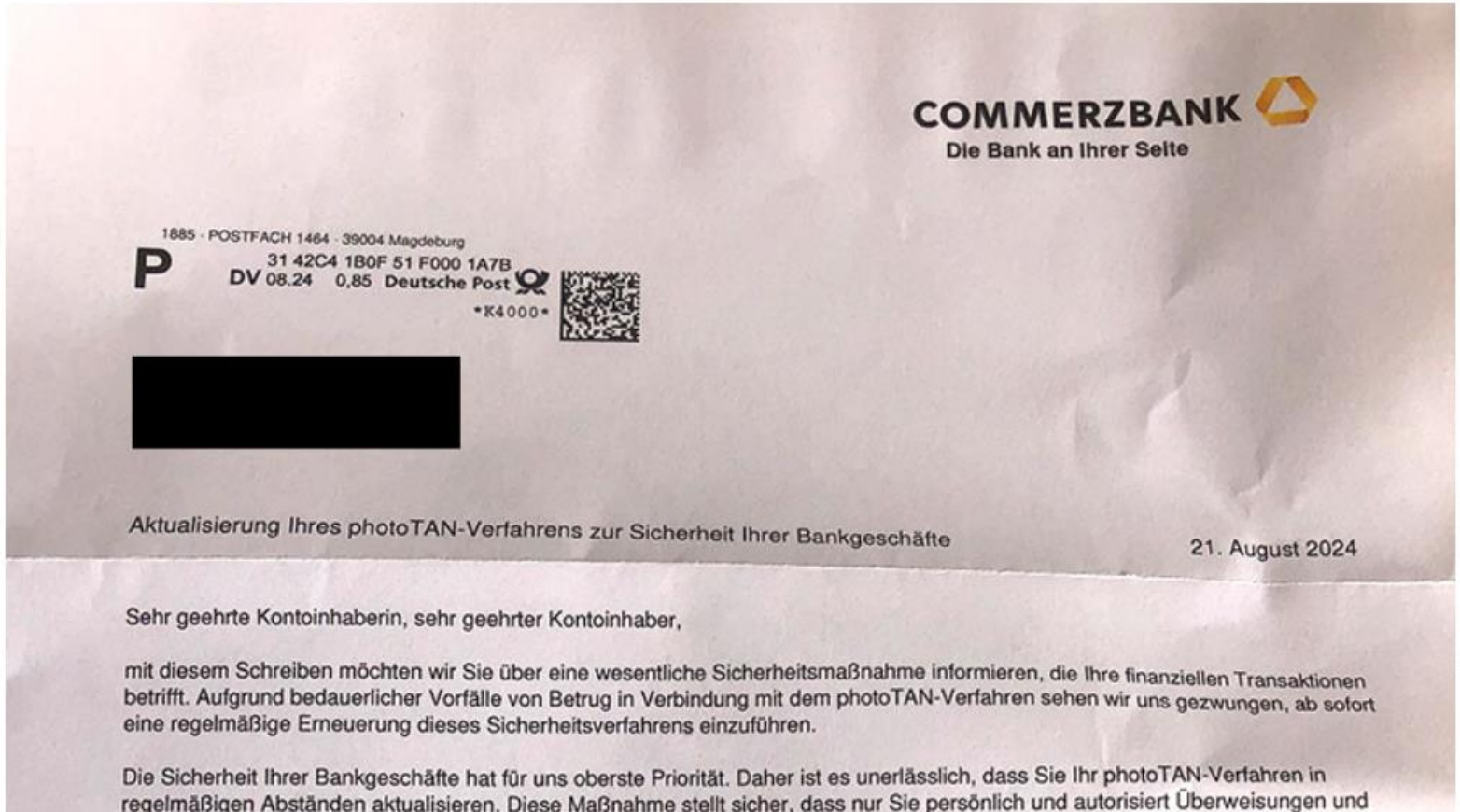
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

verbraucherzentrale Nordrhein-Westfalen

Kontakt Beratung Shop Presse Karriere Bildung Menü

manchen Fällen werden auf diese Weise direkt Geldtransfers veranlasst, warnt das **Landeskriminalamt Nordrhein-Westfalen**.

Diesen Brief hat die Münchnerin erhalten und den QR-Code in der Mitte abgedeckt:



COMMERZBANK
Die Bank an Ihrer Seite

1885 · POSTFACH 1464 · 39004 Magdeburg

P 31 42C4 1B0F 51 F000 1A7B
DV 08.24 0,85 Deutsche Post
K4000

[redacted]

Aktualisierung Ihres photoTAN-Verfahrens zur Sicherheit Ihrer Bankgeschäfte 21. August 2024

Sehr geehrte Kontoinhaberin, sehr geehrter Kontoinhaber,

mit diesem Schreiben möchten wir Sie über eine wesentliche Sicherheitsmaßnahme informieren, die Ihre finanziellen Transaktionen betrifft. Aufgrund bedauerlicher Vorfälle von Betrug in Verbindung mit dem photoTAN-Verfahren sehen wir uns gezwungen, ab sofort eine regelmäßige Erneuerung dieses Sicherheitsverfahrens einzuführen.

Die Sicherheit Ihrer Bankgeschäfte hat für uns oberste Priorität. Daher ist es unerlässlich, dass Sie Ihr photoTAN-Verfahren in regelmäßigen Abständen aktualisieren. Diese Maßnahme stellt sicher, dass nur Sie persönlich und autorisiert Überweisungen und

Kontakt
Beratung
Newsletter
Social Media
Kostenlose Online-Seminare

Veröffentlicht am 11. Juni 2025

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

mimikama.org/falscher-gerichtsvollzieher-samt-dhl-brief/

MIMIKAMA

Suchen …

Mimikama-FaktenRadar

Falsch | Vorsicht | Wahr

Mitglied werden | Clubbereich | LOGIN MIT STEADY

Falscher Gerichtsvollzieher samt DHL-Brief: Warnung vor neuer Abzocke

Täuschend echt: Betrüger setzen auf amtlichen Stil und persönliche Daten, um Druck auszuüben.

von Hildegard O. veröffentlicht am 11. Juni 2025 9:18

Offiziell wirkende Briefe täuschen viele Verbraucher

Möglichen Fake melden

Ein hochwertiges Kuvert, der Versand per DHL und ein Schreiben mit angeblichen Forderungen in Höhe von knapp 1.000 Euro: Immer mehr Menschen erhalten derzeit täuschend echte Briefe, die angeblich von einem Gerichtsvollzieher stammen. Diese Schreiben sind mit Siegeln, Unterschriften und sogar korrekt wiedergegebenen persönlichen Daten wie der eigenen Bankverbindung

Moderne Betrugsmaschen

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Quishing

Falsche QR-Codes – Online und Analog

- Bank-Briefe
- Ladesäulen und Parkautomaten
- Plakate im ÖPNV

Einreise (ETA) nach Großbritannien

Betrügerische oder überteuerte Internetseiten

- Betrügerische überteuerte Webseiten
- Prominente Platzierung in den Suchergebnissen
- Statt 10 GBP (12,- €) bsp. 70 – 200 GBP für Einreise
- (plus) Datendiebstahl

PayPal-Gastzahlung

Funktion „Gast-Zahlung“ wird für Betrug genutzt

- Gastzahlung bei PayPal ohne eigenes Konto möglich
- Kriminelle nutzen gestohlene Konto-Daten
- IBAN genügt
- Präventionshinweise → Verbraucherzentrale NRW / LKA NRW

Bild: Adobe Stock Polizei NRW

Moderne Betrugsmaschen

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Online-Marktplätze

Betrugsmasche „Sicher bezahlen“

- Kriminelle schlagen diese Zahlungsmethode vor
- Gefälschte E-Mails zum Bestätigen des Bezahlvorgangs
- Gefälschte E-Mail zum Abruf des Kaufpreises

Dreiecksbetrug

Variante A

- Drei beteiligte Personen (1x Täter/in, 2x Geschädigte)
- Betrüger/in „kassiert“ und bestellt Ware bei seriösem Händler
- Seriöser Händler schickt Ware an betrogene Person mit „weiterer“ Rechnung

Variante B

- Betrüger/in kopiert Inserat von Online-Marktplatz
- Kopiertes Inserat wird wo anders eingestellt
- Käufer/in zahlt an Original-Anbieter
- Original-Anbieter schickt Ware an Betrüger/in

Bild: Adobe Stock Polizei NRW

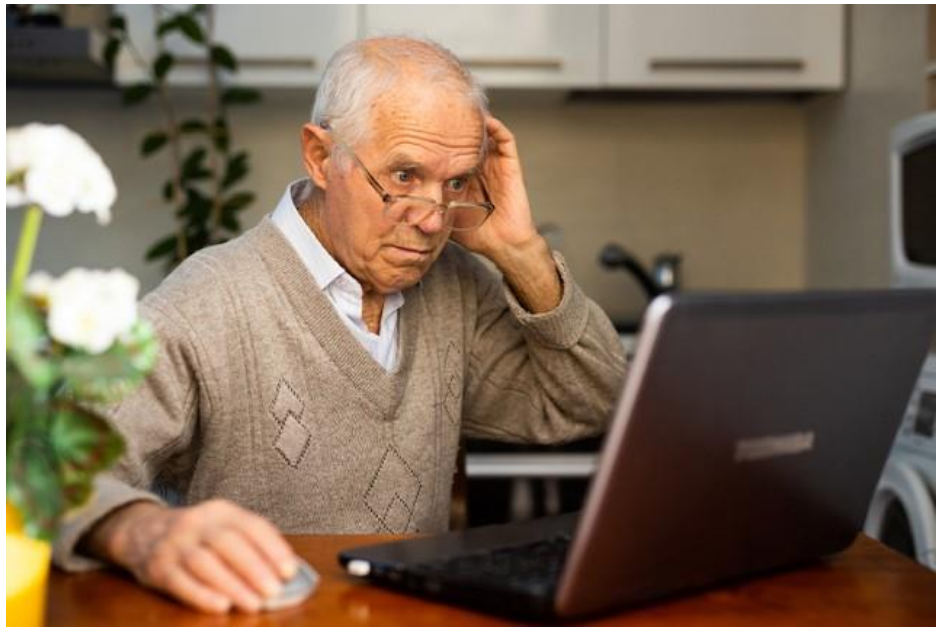
Phishing via „Sicher bezahlen“ Funktion

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

- Kontaktaufnahme mit potentiellen Geschädigten (häufig auch über gekaperte Benutzerkonten Dritter mit positiver Bewertung).
- Interesse an Inserat vortäuschen und mit GES auf Verkaufspreis einigen.
- Dem Geschädigten vorschlagen, die Zahlung über die Funktion „Sicher bezahlen“ durchzuführen.

„Wer ist so blöd und fällt darauf rein?“

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



Betrug kann jeden treffen!

Es kommt auf die Situation an.

- Angst, Stress, Sorge
- Zeitdruck
- Vertrauen
- Hilfsbereitschaft

Schuld sind nicht die Opfer, sondern immer die Täter!

Bild: Adobe Stock Polizei NRW


VICTIM BLAMING
Was ist das eigentlich?
Täter-Opfer-Umkehr ist ein Begriff aus der Kriminologie und bezieht sich auf eine Situation, in der das Opfer einer Straftat als Täterin oder Täter, bzw. als Mittäterin, Mittäter dargestellt oder behandelt wird. Der englische Begriff „Victim Blaming“ bedeutet wörtlich übersetzt „Opfer beschuldigen“ bzw. „Opfer-Schelte“. Victim Blaming tritt u.a. infolge von häuslicher Gewalt, Vergewaltigungen, klassischen Betrugsdelikten oder rassistischen Übergriffen auf. Die Ursache für einen Übergriff wird hierbei nicht bei der Tatperson, sondern im vermeintlich „provokativen“ Verhalten des Opfers gesucht.

Bild: ProPK

Cybertrading Fraud

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Wir wollen, dass Sie sicher leben. Ihre Polizei

POLIZEILICHE
KRIMINALPRÄVENTION
DER LÄNDER UND DES BUNDES

Vorsicht vor Online-Anlagebetrug

02.12.2020

Trading-Scam: Vorsicht vor Online-Anlagebetrug

21.07.2023

https://polizei.nrw/artikel/anlagebetrug-ein-andauerndes-phaenomen-mit-hohen-schadenssummen

Bild: LKA NRW

Cybertrading Fraud (Online-Geldanlage)

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

VICTIM BLAMING

Was ist das eigentlich?

Täter-Opfer-Umkehr ist ein Begriff aus der Kriminologie und bezieht sich auf eine Situation, in der das Opfer einer Straftat als Täterin oder Täter, bzw. als Mittäterin, Mittäter dargestellt oder behandelt wird. Der englische Begriff „Victim Blaming" bedeutet wörtlich übersetzt „Opfer beschuldigen" bzw. „Opfer-Schelte". Victim Blaiming tritt u.a. infolge von häuslicher Gewalt, Vergewaltigungen, klassischen Betrugsdelikten oder rassistischen Übergriffen auf. Die Ursache für einen Übergriff wird hierbei nicht bei der Tatperson, sondern im vermeintlich „provokativen" Verhalten des Opfers gesucht.

- Geschickte u. professionelle Werbung
- Betrug kann sich über mehrere Monate hinziehen
- Anfängliche Gewinne
- Persönliche Beratung und Unterstützung
- Beziehungs-/ Vertrauensaufbau
- Motivation zu höheren Investitionen
- Einsatz von Remote Software (Fernzugriff auf PC)

Bilder: Adobe Stock Polizei

https://www.watchlist-internet.at/news/deepfake-videos-mit-bekannten-gesichtern-locken-in-investmentfallen/

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Deepfake-Videos mit bekannten Gesichtern locken in Investmentfallen

Kriminelle greifen bei der Bewerbung betrügerischer Finanzangebote besonders tief in die Trickkiste. Website-Kopien von Zeitungen mit gefälschten Promi-Artikel kennen wir nur zu gut. Mittlerweile kommen aber auch zum Teil sehr professionelle Deep-Fake-Videos zum Einsatz. Darin erklären Ihnen bekannte Promis, Moderator:innen oder Politiker:innen, wie Sie mit einer „geheimen" Plattform schnell reich werden.

Cybertrading Fraud

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Trading-Scam: Vorsicht vor Online-Anlagebetrug

21.07.2023

Tinder-Trading-Scam: Lockvögel (um)werben in sozialen Netzwerken

Beim sogenannten "**Tinder-Trading-Scam**" treten **Lockvögel** zunächst über Partnerbörsen und soziale Netzwerke, wie Tinder, Badoo oder Grindr, LinkedIn oder Facebook, mit ihren potenziellen Opfern in Kontakt. Sie flirten, **versuchen Interesse zu wecken und über die Chats Vertrauen aufzubauen**. Gelingt dies, inszenieren sie sich als wohlwollender Freund oder Geschäftskontakt. Im Folgenden locken sie, angebliche Verwandte oder Bekannte aus deren Umfeld, die Opfer auf **vorgeblich besonders lukrative Anlagenportale**. Von der ersten Kontaktaufnahme bis zum "**Tippgeben**" vergehen oft mehrere Wochen.

Datenklau per Remote-Software

Die Kriminellen, die sich sehr überzeugend und selbstbewusst als echte Broker ausgeben, nutzen zudem oft eine sogenannte **Remote-Software**. Diese wird unter dem Vorwand benutzt, den Kunden das Benutzerkonto zu erklären und einzurichten. Währenddessen stehlen die Betrüger unbemerkt Daten z.B. zu Kreditkarten und Bankkonten vom PC des "Kunden". Mit den so erlangten Zugangsdaten überweisen die Betrüger später ohne Wissen der Geschädigten weitere Beträge an sich, meist auf ausländische Konten.

Mehr zum Thema

» Kredit- und Anlagebetrug

Quelle. ProPK

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Wissen schützt

T k a

Traue keinem anderen

Stoppen Hinterfragen Schützen

Verhalten im Schadenfall

Bei akuter Bedrohung Tel.: 110 wählen (Notruf der Polizei)!

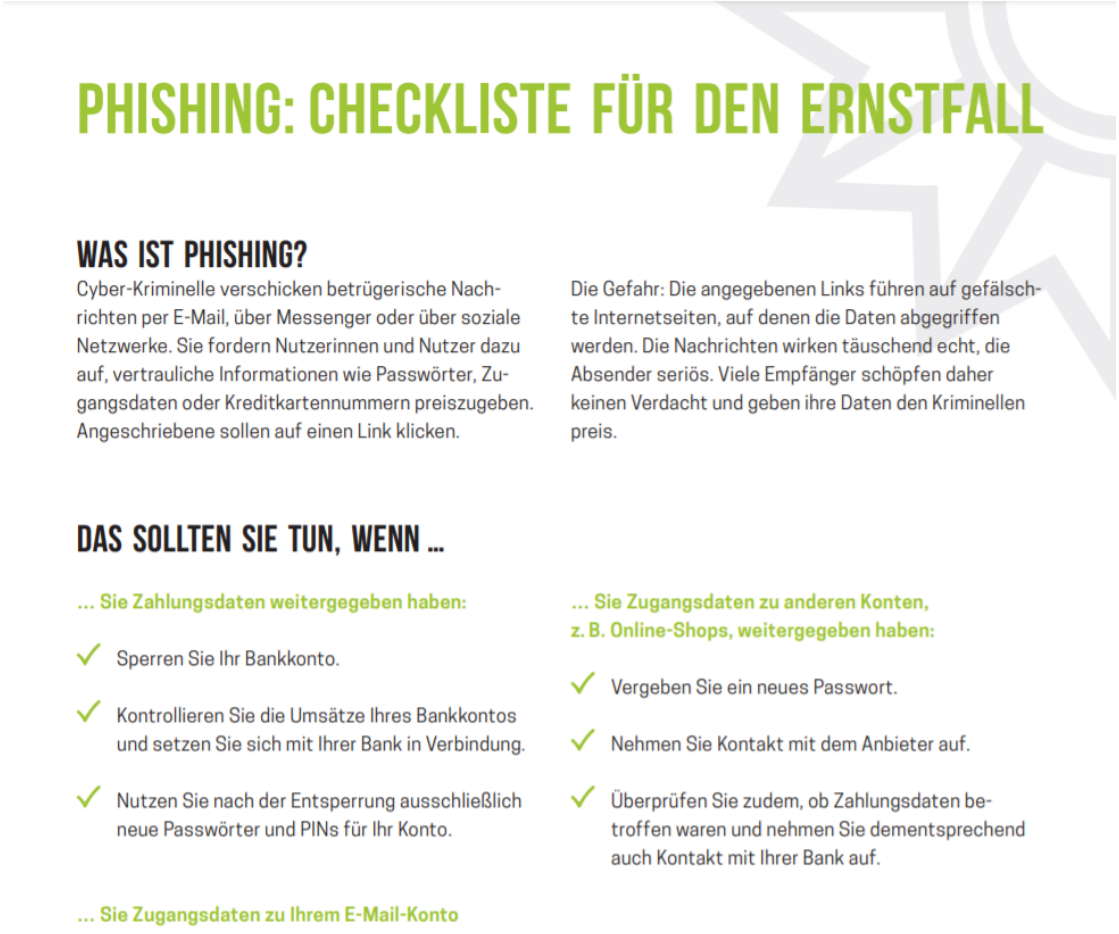
Zeigen Sie Straftaten an. Das ist bei jeder Polizeidienststelle oder online möglich!

Existierendes Datenmaterial sichern, z. B. mit Screenshots.

Erstellen Sie schon vorher Checklisten für den Ernstfall.

Checklisten für den Ernstfall

https://www.polizei-beratung.de/fileadmin/Dokumente/Phishing-Schutz-Checkliste-Ernstfall-BSI-ProPK.pdf



PHISHING: CHECKLISTE FÜR DEN ERNSTFALL

WAS IST PHISHING?

Cyber-Kriminelle verschicken betrügerische Nachrichten per E-Mail, über Messenger oder über soziale Netzwerke. Sie fordern Nutzerinnen und Nutzer dazu auf, vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern preiszugeben. Angeschriebene sollen auf einen Link klicken.

Die Gefahr: Die angegebenen Links führen auf gefälschte Internetseiten, auf denen die Daten abgegriffen werden. Die Nachrichten wirken täuschend echt, die Absender seriös. Viele Empfänger schöpfen daher keinen Verdacht und geben ihre Daten den Kriminellen preis.

DAS SOLLTEN SIE TUN, WENN ...

... Sie Zahlungsdaten weitergegeben haben:

- ✓ Sperren Sie Ihr Bankkonto.
- ✓ Kontrollieren Sie die Umsätze Ihres Bankkontos und setzen Sie sich mit Ihrer Bank in Verbindung.
- ✓ Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter und PINs für Ihr Konto.

... Sie Zugangsdaten zu anderen Konten, z. B. Online-Shops, weitergegeben haben:

- ✓ Vergeben Sie ein neues Passwort.
- ✓ Nehmen Sie Kontakt mit dem Anbieter auf.
- ✓ Überprüfen Sie zudem, ob Zahlungsdaten betroffen waren und nehmen Sie dementsprechend auch Kontakt mit Ihrer Bank auf.

... Sie Zugangsdaten zu Ihrem E-Mail-Konto

Quelle: ProPK

Hilfreiche Internetseiten

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

www.polizeiberatung.de

www.mach-dein-passwort-stark.de

www.susii.nrw

www.bsi-fuer-buerger.de

www.verbraucherzentrale.nrw

www.bagso.de/themen/digitalisierung/

Betrug und KI (Deepfake)

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

AI Scambaiters: O2 creates AI Granny to waste scammers' time

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Danke für Ihre Aufmerksamkeit

Landeskriminalamt Nordrhein-Westfalen
Abt. 3 - Dezernat 32 – Sachgebiet 32.1
Kriminalprävention und Opferschutz

Stefanie Lösing
Kriminalhauptkommissarin
Tel.: 0211-939-3217
Fax: 0211-982-193212
Stefanie.Loesing@polizei.nrw.de