POLIZEI

KRIMINALPRÄVENTION

Internetkriminalität

Obereder/Castrol Unternehmertag 2025

POLIZEI

KRIMINALPRÄVENTION

Internetkriminalität

Entwicklung Österreich – angezeigte Fälle

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	10.010	4.157	41,5%
Jahr 2016	13.103	5.072	38,7%
Jahr 2017	16.804	6.470	38,5%
Jahr 2018	19.627	7.332	37,4%
Jahr 2019	28.434	10.187	35,8%
Jahr 2020	35 915	12.012	33,4%
Jahr 2021	46.179	17.020	36,9%
Jahr 2022	60.195	20.378	33,9%
Jahr 2023	65.864	20.818	31,6%
Jahr 2024	62.328	19.785	31,7%
Veränderung	-5,4%	-5,0%	0,1%-Punkte

Quelle: Polizeiliche Kriminalstatistik 2024

POLIZEI

KRIMINALPRÄVENTION

Internetbetrug

Angezeigte Fälle Ö

Internetbetrug	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	7.473	3.034	40,6%
Jahr 2016	9.672	3.909	40,4%
Jahr 2017	11.761	4.592	39,0%
Jahr 2018	13.328	4.956	37,2%
Jahr 2019	16.831	6.382	37,9%
Jahr 2020	18.780	6.626	35,3%
Jahr 2021	22.440	8.348	37,2%
Jahr 2022	27.629	9.814	35,5%
Jahr 2023	34.069	10.472	30,7%
Jahr 2024	31.768	9.799	30,8%
Veränderung	-6,8%	-6,4%	0,1%-Punkte

Quelle: PKS 2024

Internetbetrug

Häufigste Modi Operandi (generell / insgesamt)

- Bestellbetrug („Marktplatz Internet“)
- Vorschussbetrug (Gewinn-, Erbschafts- Liebesversprechen, gefälschte Online-Shops, Immobilienagenturen, Speditionen usw…)
- Anlagebetrug (Online-Trading, meist Kryptowährung…)
- Telefonbetrug (Anrufbetrug – falsche Polizisten, Technical Support…., SMS-WA Trick…..)
- **Vielfach in Verbindung mit Phishing**

POLIZEI

Internetbetrug

„PHISHING“

Internetbetrug

Phishing

- Oft in Kombination zu Betrugs- Erpressungshandlungen
- Erweiterte Formen („Credential-Stuffing“, „Brute-Force“)
- **Ziele: Sensible Daten, vertrauliche Informationen**
- **Mit den Daten werden weitere Straftaten verübt**
- **Unterschiedliche Tatmittel** (E-Mail, SMS, Soziale Netzwerke…)

Internetkriminalität

Angriffsziel: Unternehmen = MA od. Kunden

(Einige M.O.)

- Phishing / (unterschiedliche M.O.)
- Social Engineering

..Erstangriff, welcher weitere Angriffe ermöglicht…..

- CEO-Fraud, BEC
- Betrügerische Zahlungs- od. Überweisungsaufträge
- Betrügerische Warenbestellungen
- Einschleusen Schadsoftware

Angriffe auf Unternehmen

Szenarien

Angriffsziel: Unternehmen

- Direkt (z.B. DDoS, Malware…)
- Indirekt (Angriff über Mitarbeiter od. Kunden (Achtung: „Social Engineering“)

Angriffsziel: MA („Phishing“, „Social Engineering“)

- Firmendaten und Abläufe werden ausgekundschaftet
- Zugangsdaten, Geld herausgelockt
- Schadsoftware eingeschleust

Angriffsziel: Kunde

- Opfer von Betrug, ID-Diebstahl ……
- „Money-Mules“ (Geldwäsche)

POLIZEI

KRIMINALPRÄVENTION

Erpressung im Internet

„RANSOMWARE“

⚠ Meist E-Mail als Köder

⚠ Lösegeld-Forderung

Internetkriminalität

Angriffe auf Unternehmen

Lücken im Bereich IT-Security

– Technische Lösungen

Menschliche Schwachstellen

– Achtung: Größtes Cyberrisiko – **Social Engineering**

– MA sensibilisieren / informieren!!

POLIZEI

KRIMINALPRÄVENTION

„Schwachstelle Mensch“

…Schäden im Unternehmen und Privat

Angriffsziel: Unternehmen

- Direkt (z.B. DDoS, Malware…)
- Indirekt (Angriff über Mitarbeiter od. Kunden (Achtung: „Social Engineering“)

Angriffsziel: MA

- Firmendaten, Abläufe
- Zugangsdaten – auch private, Geld **(Betrug, Erpressung)**
- Schadsoftware einschleusen

Angriffsziel: Kunde

- Opfer von **Betrug, Erpressung**, ID-Diebstahl ……
- „Money-Mules“ (Geldwäsche)

Internetbetrug

Häufigste Modi Operandi (generell / insgesamt)

- Bestellbetrug („Marktplatz Internet“)
- Vorschussbetrug (Gewinn-, Erbschafts- Liebesversprechen, gefälschte Online-Shops, Immobilienagenturen, Speditionen usw…)
- Anlagebetrug (Online-Trading, meist Kryptowährung…)
- Telefonbetrug (Anrufbetrug – falsche Polizisten, Technical Support…., SMS-WA Trick…..)
- **Vielfach in Verbindung mit Phishing**

Internetbetrug

Bestellbetrug

- Verkäufer / od. Käufer als Täter
- „Dreiecksbetrug“

Anlagebetrug

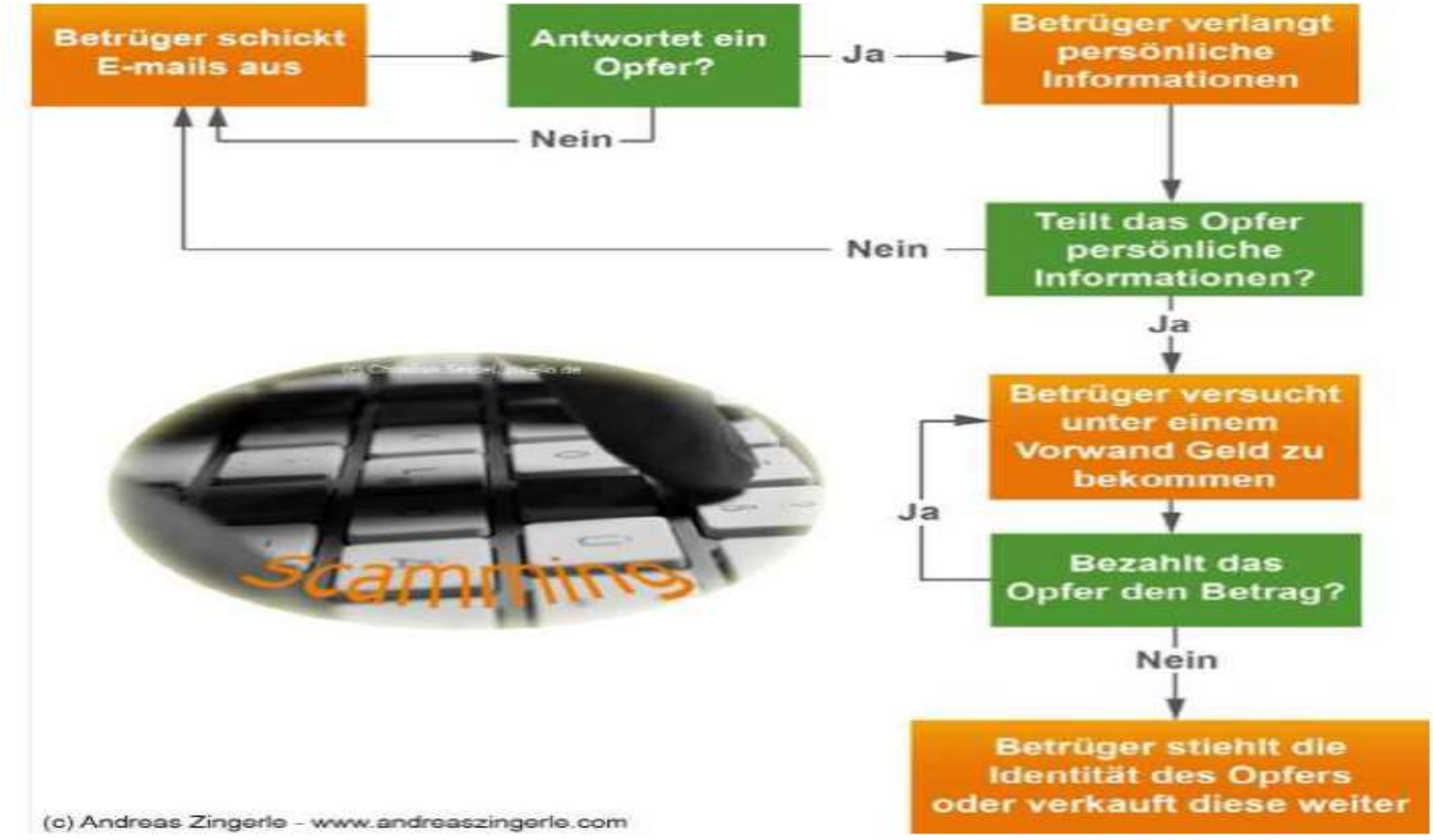
- Versprechen hoher Rendite
- Anlage angebl. in Kryptowährung od. Rohstoffe
- Geringe „Einstiegszahlung“ / als Köder
- Gefälschte Websites
- Kommunikation / Manipulation

POLIZEI

KRIMINALPRÄVENTION

„Vorschussbetrug“

Typischer Ablauf



POLIZEI

KRIMINALPRÄVENTION

„Vorschussbetrug“

Beispiel „Gewinnversprechen“

Loterías y Apuestas del Estado

EL GORDO LOTO INTERNATIONAL VERLOSUNG S.A.

C/SAN PEZ ANCATARA 24.
08905, BARCELONA – SPAIN
OFFIZIELLE MITTEILUNG
VON SITZ DES VIZE PRASIDENTEN.

22 /05/2017

ACHTUNG: BEGÜNSTIGTER.

OFFIZIELLE GEWINNBENACHRITIGUNG

Wir sind erfreut ihnen mitteilen zu konnen, das die gewinnliste LOTERIAL NACIONAL an 22/ 04/ 2017 erschienen ist.Dir offizielle liste der gewinner erschien am 22/ 05/ 2017 Ihr email id wurde auf dem los mit dir nummer: 99.11464992.221 und mit der seriennummer:0016-17, Ref N° EG/7052556103/17 und stapel n°:NL/14/667/2EL registried. Die glucksnummer: 23-16-88-46, haben in der 2. Kategorie gewonnen.

Sie sind damit gewinner von: €825, 000,00 (ACHT HUNDERT UND FÜNF UND ZWANZIG TAUSEND EUROS NUR.) Die summe ergibt sich einer gewinnausschuttung von €9,900.000 (NEUN MILLIONEN NEUN HUNDERT TAUSEND EUROS NUR) Geteilt unter den zwölf internationalen Gewinnern in ihren jeweiligen Kategorien.

HERZLICHEN GLUCKWUNSCH!!!

Dir gewinn ist bei einer sicherheitsfirma hinterlegt und in ihren namen versichert. um keine komplikationen bei der abwicklung der zahlung zu verursachen bitten wir sie diese offizielle mitteilung , diskret zu behandeln.,es ist ein teil unseres sicherheitsprotokolls und garantiet ihnen einen reibunglosen Ablauf.Alle gewinner werden per computer aus 45.000 namen aus ganz europa ,asien, australien und amerika als teil unsererInternationalen promotion programms ausgewahlt, Welches wir einmal im jahr veranstalten.

Bitte kontaktieren sie unseren auslands sachbearbeiter DR, FERNANDEZ LOPEZ, bei der sicherheitfirma SANTALUCIA SEGUROS S.L. On Tel:0034 672 958 437, Fax: 0034 912 919 546,E-Mail: santa_luciaseguros@spainmail.com. Für die Verarbeitung und die Geldüberweisung von Ihrem siegreichen Preisgeld zu Irgendeiner Bezeichnung von Ihrer Wahl Bitte denken sie daran, jeder gewinnanspruch muss bis zum 21/08/2017 Angemeldete sein. Jeder nicht angemeldet Gewinnanspruch verfallt und geht zuruck an das MINISTERIUM DER FINANZ. Als nicht beansprucht. Und auch wird informiert, dass 10% von Ihrem Lotteriengewinn SANTALUCIA SEGUROS S.L gehört Ein. geht. Dir 10% sind erst nach erhalt des gewinnes fallig da der gewinn in ihren namen versichert ist.

WICHTIG: um verzogerungen und komplikationen zu vermeiden, bitte immer referenznummer und bearbeitungsnummer angeben. Adressanderungen bitte immer so schell wie moglich mitteilen Anbei ein anmeldeformular, bitte ausfullen und zuruck

DON LUIS ALBERT
(VICE PRESIDENT INTERNACIONAL AWARD DEPT.)

Telefonbetrug

Anrufbetrug

- Falsche Polizisten / Staatsanwälte
- Technical Support
- Falsche Behörden

- Call-ID Spoofing

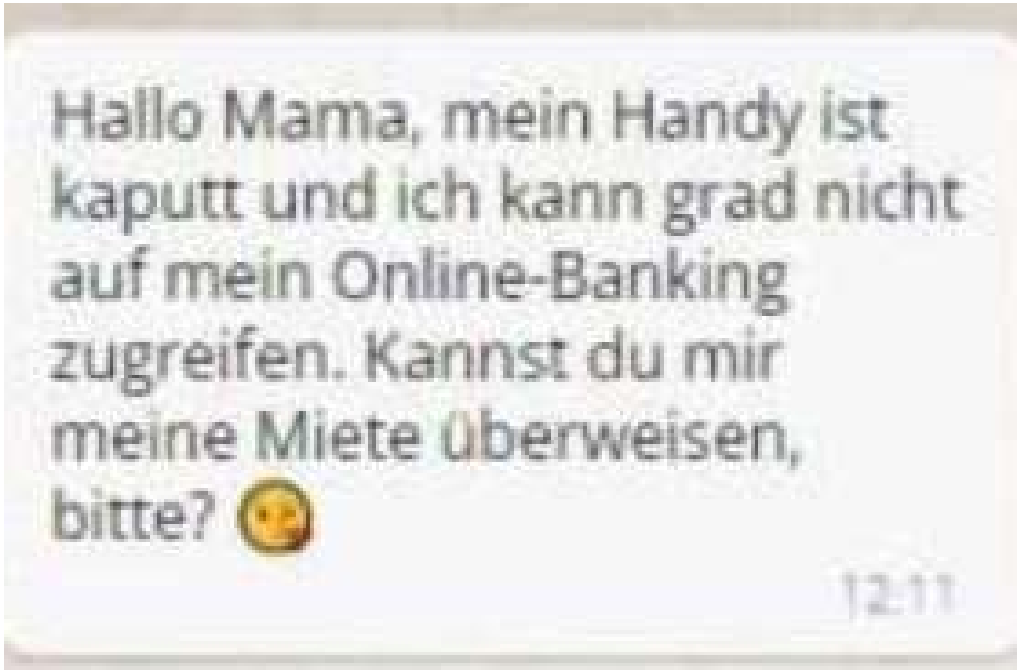
© pixarbay.com

POLIZEI

KRIMINALPRÄVENTION

Telefonbetrug

„SMS – WA – Trick“



Internetkriminalität

Angriffsziel: Unternehmen

Prävention

© pixabay.com

- IT-Sicherheitssysteme (u.a. Datensicherungen, IP-Monitoring – z.B. Erkennen von automatisierten Anmeldeversuchen od. DDoS-Attacken durch Bot-Netze)
- Abläufe (u.a. „Clean Desk“, externe Datenträger, E-Mails prüfen / verifizieren)
- Informationspolitik (intern, MA sensibilisieren, Web-Auftritt)

Internetkriminalität

Prävention

- Kunden informieren / warnen
- Weitere Informationen:
  www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx

Internetkriminalität

Wenn‘s passiert

Anzeige Polizei

- Beweismittel, Datenmaterial sichern (Originalzustand)
- Leitfaden unter: Publikation des Bundes (bundeskriminalamt.at)

- Weitere Hilfestellung (z.B. „The No More Ransom Project”)