POLIZEI
Nordrhein-Westfalen
Kreis Coesfeld

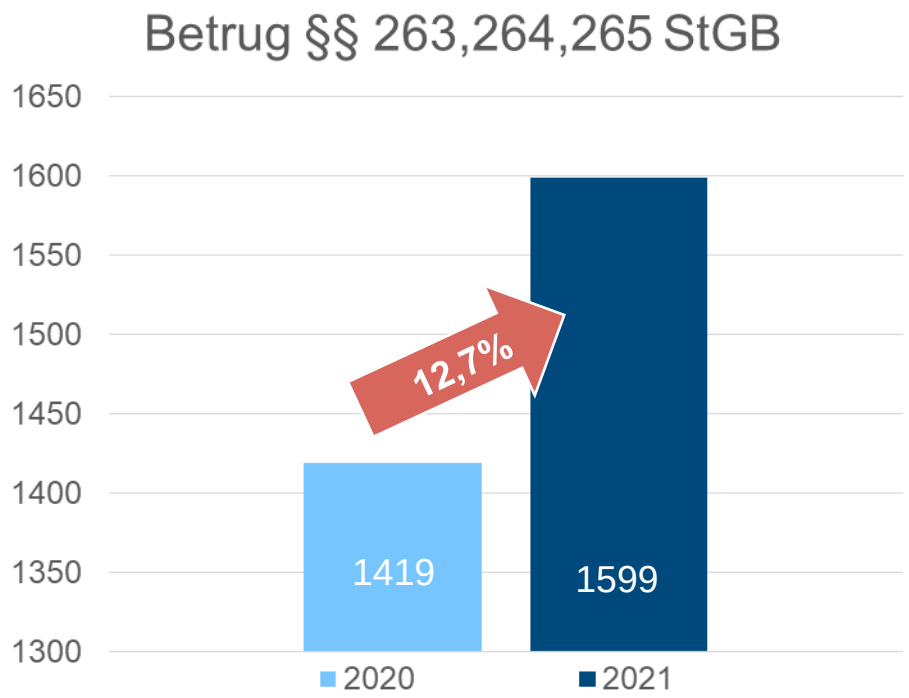
bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Neue Wege der Kriminalität

Zahlen und Daten

- Waren-, Warenkreditbetrug
- Computerbetrug
- Kapitalanlagebetrug
- Kreditbetrug



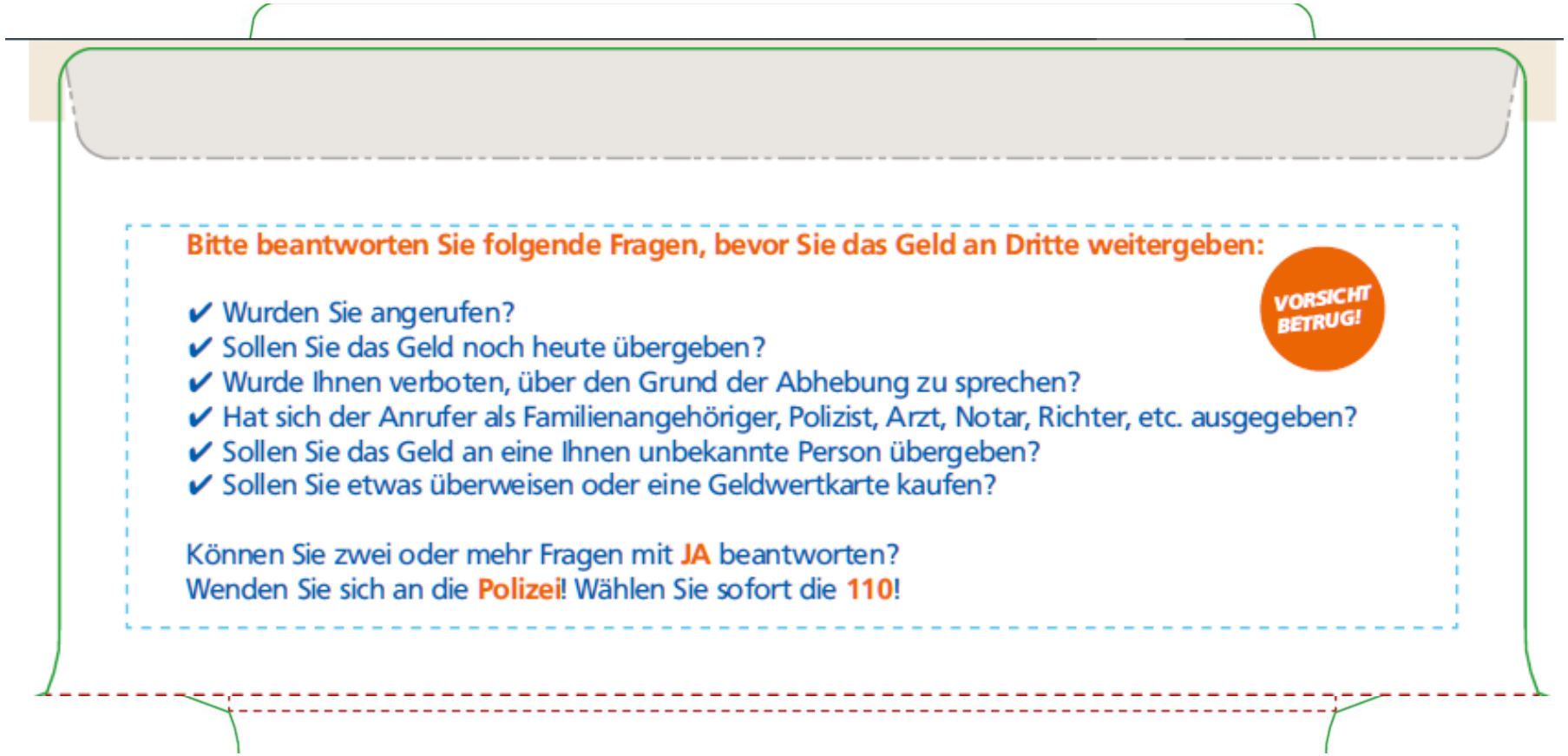
Quelle: Polizeiliche Kriminalstatistik 2021

Betrug an Senioren im Kreis Coesfeld

2020: 790 Fälle, davon 24 erfolgreich

Schaden: 389.485 €

Prävention bei Geldauszahlungen



Definition „Cybercrime“

- international einheitliche Beschreibung für Computerkriminalität
- umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden
- der Computer kann sowohl Werkzeug als auch Ziel eines Angriffs sein, am häufigsten unter Verwendung des Tatmittels Internet


POLIZEILICHE KRIMINALSTATISTIK 2021
COMPUTERKRIMINALITÄT
erfasste Fälle
35.000
30.000
25.000
20.000
15.000
10.000
5.000
0
22.708
22.913
19.693
20.118
24.294
30.115
+ 24 %
2016
2017
2018
2019
2020
2021
MINISTERIUM DES INNERN
Computerkriminalität im Sechs-Jahres-Vergleich

Um was für eine Straftat im Internet handelte es sich?

Jeder 4.
war schon einmal Opfer von Cyberkriminalität

Quelle: Digitalbarometer 2021

Enkeltrick über WhatsApp

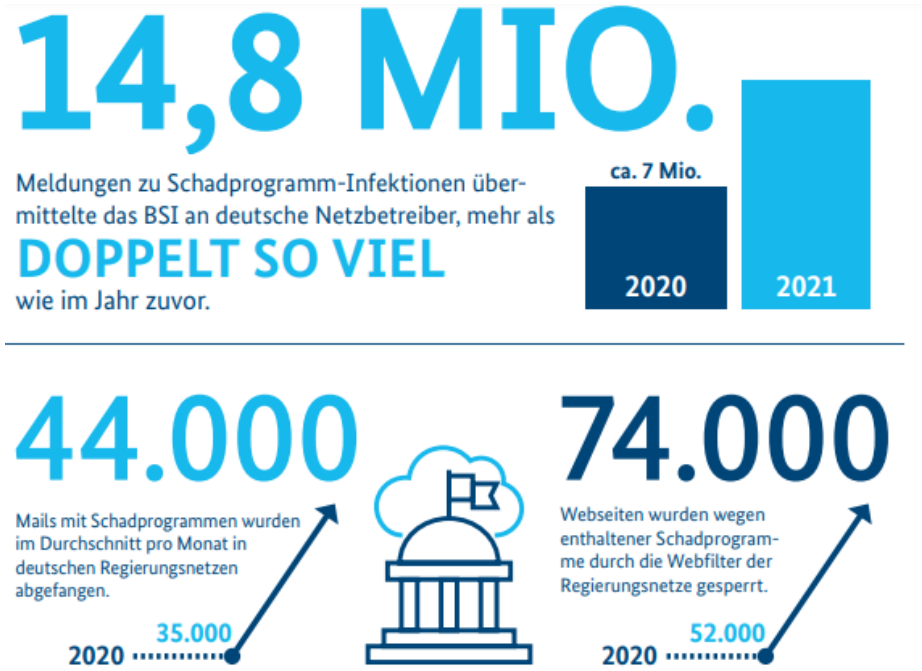
Microsoft Support Mitarbeiter (Tech-Support-Scam)

Anruf eines Microsoft-Mitarbeiters
Probleme auf ihrem Gerät sollen behoben werden

Fernwartung – Bedarf ihrer Zustimmung
Ziel: Zugang zu ihrem Gerät und allen gespeicherten Passwörtern z.B. Online-Shops

Bezahlung des Services per Bitcoin
Abschluss eines Vertrages mit Bitcoin-Firma z.B. Bitpanda
Ziel: Sie zahlen die Bitcoin und Schulden der Firma den Betrag

Schadprogramme



Quelle: BSI Lagebild Cybercrime 2021

Risiken der Informationstechnik (Unternehmen)

- Datendiebstahl durch Hackergruppen
- Datenverlust durch technische Schäden oder Verschlüsselung durch Schadsoftware
- Datenmissbrauch durch den Verkauf an Konkurrenzfirmen
- Häufiger Angriffspunkt: Mitarbeitende

10 Punkte für eine sicher Infrastruktur (Unternehmen)

1. Sensibilisierung der Mitarbeiter
2. Backups
3. Netzwerksegmentierung
4. Firewall
5. Virenschutz
6. Softwareaktualisierungen
7. Nutzerprofile
8. Siche Passwörter
9. IT-Notfallpläne
10. IT-Dienstleister

Vorsicht, Phishing! Betrügerische E-Mails erkennen

Gefälschte Absender-Adresse
Ist die E-Mail-Adresse des Absenders z.B. durch einen Vergleich zu verifizieren? Kann der Absender den Versand der Mail persönlich/ telefonisch bestätigen?

Abfrage vertraulicher Daten
Fordert die E-Mail zur Eingabe persönlicher Informationen auf? Werden Geheimnummern oder Passwörter abgefragt?

Vorgetäuschter dringender Handlungsbedarf
Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf? Wird eine Nachricht des Absenders erwartet?

Links zu gefälschten Webseiten
Enthält die E-Mail Verlinkungen, die auf andere Webseiten verweisen? Welche Ziel-URL wird bei einem Mouseover angezeigt?

Sprachliche Ungenauigkeiten
Ist die Anrede unpersönlich formuliert? Enthält der Text Rechtschreib- oder Zeichenfehler?

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Vishing

Telefonbetrug: Abgreifen von Daten mittels fingierter Bank-Anrufe

Smishing

SMS-Betrug: Abgreifen von Daten per Textnachrichten in Namen einer Bank

Künstliche Intelligenz

- es gibt viele technische Möglichkeiten Bilder und Videos zu verändern
- „Deepfakes“ - Fotos und Videos von Personen können generiert werden
- mittlerweile auch in Echtzeit – d.h. während die Kamera läuft können Bild und Ton verfremdet werden

→an „kleinen Fehlern“ in den Bildern können Sie die Bearbeitung erkennen

Cybergrooming

- die gezielte Anbahnung sexueller Kontakte mit Minderjährigen über das Internet

- häufig geben Täter*innen sich als Kinder, Jugendliche oder junge Erwachsene aus um Vertrauen aufzubauen

- Ziel ist in den meisten Fällen eine sexuelle Belästigung bis hin zum sexuellen Missbrauch in der Realität – *bereits der Versuch ist strafbar!*
  - *„hübsches Lächeln – ich könnte Modelfotos von dir machen“*
  - *„ich finde dich so hübsch, schick doch mal ein Bild oben ohne“*
  - *„das ist unser Geheimnis“*

Sexting

- zusammengesetzt aus „sex“ und „texting“

- Versenden von Textnachrichten, freizügigen Bildern oder Nacktbildern über Messengerdienste wie Snapchat, WhatsApp, Skype und Co.

- Sexting ist strafbar wenn
  - Bilder von unter 14 Jährigen oder an diese versendet werden
  - Bilder ohne Einverständnis weiterversendet/veröffentlicht werden

Hate Speech

- Hassrede in der digitalen Welt beleidigt, bedroht und verachtet Menschen aufgrund ihrer Herkunft, ihres Glaubens, ihres Geschlechts oder ihrer sexuellen Orientierung

  → Bilder, Videos und Kommentare

- Netzwerkdurchsetzungsgesetz (NetzDG)
  - 2017: Verfahren zum Umgang mit Beschwerden
  - 2022: Meldepflicht ans Bundeskriminalamt (BKA)

Verbotene Inhalte

- Illegale Downloads
- Gewaltverherrlichende Fotos und Videos
- extremistische Inhalte, die zu Hass und Gewalt auffordern
- Symbole verfassungswidriger Organisationen
- Besitz und Verbreitung von kinderpornografischen Bildern und Videos

Rechtliches

Gesetzliche Neuerungen zur Sexualstraftaten in der virtuellen Welt (Strafandrohung)

§ 184 b Abs.1

Verbreitung KIPO

Bis
01.07.21
3 M. – 5 J.

Seit
01.07.21
1 J. – 10 J.

§ 184 b Abs. 3

Verschaffen von Aufzeichnungen

Bis
01.07.21
GS – 3 J.

Seit
01.07.21
1 J. – 5 J.

§ 184 c Abs. 1

Verbreitung von Jugendporno

Bis
01.07.21
GS – 3 J.

Seit
01.07.21
GS – 3 J.

§ 184 c Abs. 3

Erwerb/Besitz von Jugendporno.

Bis
01.07.21
GS – 2 J.

Seit
01.07.21
GS – 2 J.

Ermessensspielraum?

Vergehen

… rechtwidrige Taten welche mit einer Mindestfreiheitsstrafe von unter einem Jahr oder mit Geldstrafe bedroht sind.

Verbrechen

… rechtswidrige Taten welche mit einer Mindestfreiheitsstrafe von über einem Jahr oder darüber bedroht sind.

Problem:

Verbreiten/Besitz kinderpornographischer Inhalte (§ 184 b StGB)

- auch bei vermeintlich lustigen Bildern/Videos/Sticker

- keine Einstellung nach § 45 Abs. 1 JGG mehr möglich

- ca. 40 % der Täter nach NCMEC-Meldungen sind Jugendliche und Heranwachsende

Problem:

WhatsApp-Gruppen / Unterschiedliche Rechtsauffassung bei StA:

A

- unabhängig vom übrigen Inhalt des Gruppenchats und von Reaktionen der übrigen Teilnehmer immer Anfangsverdacht § 184 b Abs. 3 StGB

B

- abhängig vom Inhalt des Gruppenchats und von Reaktionen der übrigen Teilnehmer (als Merkmal für einen Besitzwillen)

Meinung StA ZAC Köln

* ausschließlich KiPo-Gruppe = Anfangsverdacht (+)
* negative Reaktion = kein Anfangsverdacht (-)
* keine Reaktion = kein Anfangsverdacht (-)

Problem:

WhatsApp-Gruppen / Umgang mit kritischen Inhalten:

- der nicht vorsätzliche Besitz ist straflos

  * belegt durch Vernichtung oder Ablieferung (Meinung StA ZAC Köln)
  * keine Weiterleitung / eigene Sicherung
  * Pädo-Hunter (Achtung: Verfahrensgefährdung / ggf. eigene strafbare Handlung)

Präventionstipps

- Schützen Sie Ihr/en Computer/Laptop/Smartphone
- Ein Anti-Viren-Programm und eine Firewall gehören zur Grundausstattung
- Nutzen Sie unterschiedliche Browser für verschiedene Zwecke
- Nutzen Sie kein freies WLAN

Präventionstipps

- Sollte Ihnen etwas fraglich erscheinen, so sperren Sie den Zugang
- Verwalten Sie Ihre Passwörter/Geheimzahlen sicher
- Schalten Sie Bluetooth nur an wenn Sie es benötigen
- Kleben Sie ihre Webcam ab
- Geben Sie möglichst wenig private Informationen von sich Preis

Sichere Passwörter

- mindestens 10 Zeichen
- Buchstaben, Zahlen und Sonderzeichen

- für jedes Portal ein anderes Passwort

- Passwörter niemals an andere Personen weitergeben!

Öffnungszeiten

Montag	**9:00 – 16:00 Uhr**
Dienstag	**9:00 – 17:30 Uhr**
Mittwoch	**geschlossen**
Donnerstag	**9:00 – 16:00 Uhr**
Freitag	**9:00 – 14:30 Uhr**
Jeden 2. Samstag im Monat	**9:00 – 13:30 Uhr**

So erreichen Sie uns

Bernhard-von-Galen-Str. 7a, 48653 Coesfeld

In dringenden Fällen:
Polizeinotruf 110

Polizeiwache Coesfeld
Daruper Str. 7
48653 Coesfeld

Kreispolizeibehörde Coesfeld
Daruper Str. 7
48653 Coesfeld

Tel. (02541) 14 444
poststelle.coesfeld@polizei.nrw.de
www.polizei.nrw.de/coesfeld

POLIZEI
Nordrhein-Westfalen
Kreis Coesfeld

bürgerorientiert · professionell · rechtsstaatlich

Beratungsstelle der Kriminalpolizei
für den Kreis Coesfeld

www.polizei.nrw.de/coesfeld

POLIZEI
Nordrhein-Westfalen
Kreis Coesfeld

Ihre Ansprechpartner

Technische Prävention
Andreas Nitz (02541) 14 393
Ulrike Twiehoff (02541) 14 391

Opferschutzbeauftragte/Gewaltprävention
Inga Brockmann (02541) 14 390
Katja Börsting (02541) 14 390

Kriminalität zum Nachteil von Senioren
Ulrike Twiehoff (02541) 14 391

Suchtprävention
Andreas Nitz (02541) 14 393

Cyberkriminalität
Katrin Hagedorn (02541) 14 392

Vermögen/Eigentum
Ulrike Twiehoff (02541) 14 391

Jugendschutzbeauftragter
Andreas Nitz (02541) 14 393

E-Mail Adresse:
KKVorbeugung.Coesfeld@polizei.nrw.de

HÄUSLICHE GEWALT

HATE SPEECH MOBBING

STÄDTEBAULICHE PRÄVENTION

SICHERHEIT IM ALTER

MISSBRAUCH JUGENDSCHUTZ

OPFERSCHUTZ VORTRÄGE

KRIMINALPRÄVENTION COESFELD

OPFERHILFE CYBERCRIME

STALKING

BERATUNG EINBRUCHSCHUTZ

GEWALTPRÄVENTION

SICHERHEIT AM ARBEITSPLATZ

ZUHAUSE SICHER ENKELTRICK

TASCHENDIEBSTAHL

SUCHT

NETZWERKARBEIT

INFEKTION MIT SCHADPROGRAMMEN: CHECKLISTE FÜR DEN ERNSTFALL

Ein Schadprogramm ist eine Software, die unerwünschte und meist schädliche Funktionen auf einem infizierten PC, Smartphone oder internetfähigem Gerät ausführt. Oft gelangt sie unbemerkt auf ein System, z. B. beim Surfen oder Öffnen von Dateianhängen.

Cyberkriminelle nutzen Schadsoftware als Werkzeug für Datendiebstahl, Online-Betrug oder digitale Erpressung. Täglich kommen unzählige neue Schadprogrammvarianten hinzu.

SO ERKENNEN SIE SCHADPROGRAMME

Wenn Sie einen Sperrbildschirm mit einer Zahlungsforderung sehen, handelt es sich zweifelsfrei um einen Erpressungsversuch nach einer Infektion mit einem Schadprogramm. Hinweise auf Hintergrundaktivitäten eines Schadprogramms sind auch:

Smartphones, deren Akku sich schneller entlädt, oder in Ihrem Namen versendete Spammails an Ihre Kontakte. Bereits in einer solchen Situation sollten Sie Schritte zur Überprüfung der Sicherheit Ihrer Geräte unternehmen.

DAS SOLLTEN SIE TUN, WENN …

… Sie ein Schadprogramm auf Ihrem Gerät vermuten:

- **Trennen Sie das Gerät vom Netzwerk:** Schalten Sie das WLAN aus oder entfernen Sie das Netzwerkkabel.
- **Starten Sie einen Virenscan:** Führen Sie auf dem Gerät einen Offline-Virenscan durch. Achten Sie darauf, dass Ihr Virenschutzprogramm aktuell ist.

Eine umfangreiche Schritt-für-Schritt-Anleitung für die Infektionsbeseitigung von Schadsoftware auf PC, Smartphone und Tablet sowie weiteren smarten Geräten finden Sie auf:
www.bsi-fuer-buerger.de/infektionsbeseitigung.

- **Setzen Sie das System neu auf:** Aufgrund der möglichen Änderungen am System durch das Schadprogramm sollte grundsätzlich eine Neuinstallation des Betriebssystems vorgenommen werden. Smartphone und Tablets sollten Sie auf Werkseinstellungen zurücksetzen.
- **Ändern Sie Ihre Passwörter:** Beginnen Sie mit dem E-Mail-Konto, das Sie zum Zurücksetzen anderer Passwörter benötigen. Aktivieren Sie wenn möglich eine Zwei-Faktor-Authentisierung.

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

Wir wollen, dass Sie sicher leben.
Ihre Polizei
Kompetent. Kostenlos. Neutral.

POLIZEILICHE KRIMINALPRÄVENTION
DER LÄNDER UND DES BUNDES

verbraucherzentrale
Nordrhein-Westfalen

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•