Kriminalprävention Cybercrime

Themen & Inhalte

- Definition Cybercrime
- Zahlen Cyberkriminalität
- Formen von Cybercrime
- Grundschutz & Internetsicherheit
- Schutz & Prävention

POLIZEI Nordrhein-Westfalen Dortmund

Definition Cybercrime

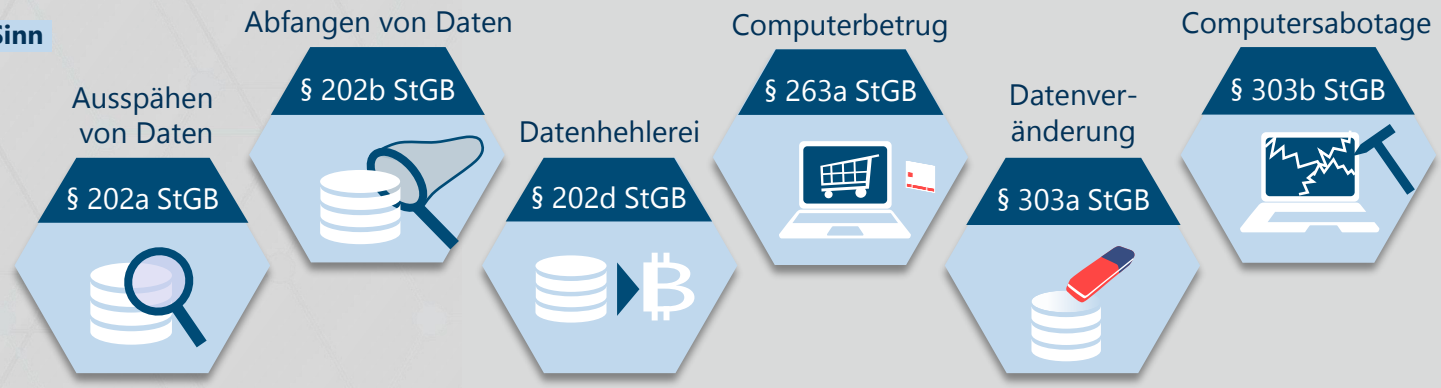
Definition Cybercrime

Der Begriff **Cybercrime** steht als international einheitliche Beschreibung für **Computerkriminalität** und umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden.

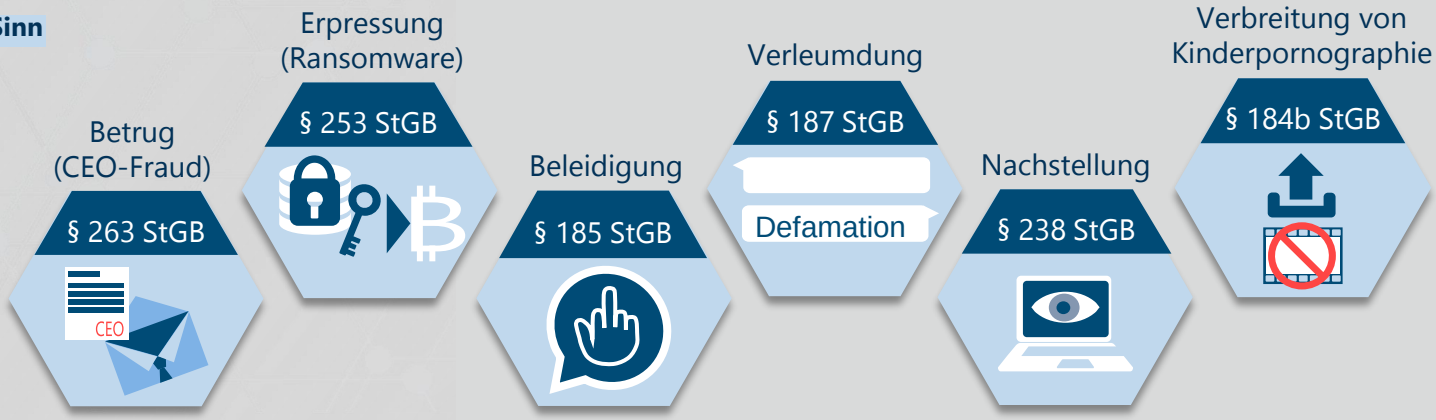
// Straftaten richten sich dabei grundsätzlich gegen das Vermögen oder die persönliche Integrität; am häufigsten unter Verwendung des Tatmittels Internet und E-Mail

Definition Cybercrime

Cybercrime im engeren Sinn
Straftaten, bei denen ein Computer als Tatwaffe eingesetzt wird.

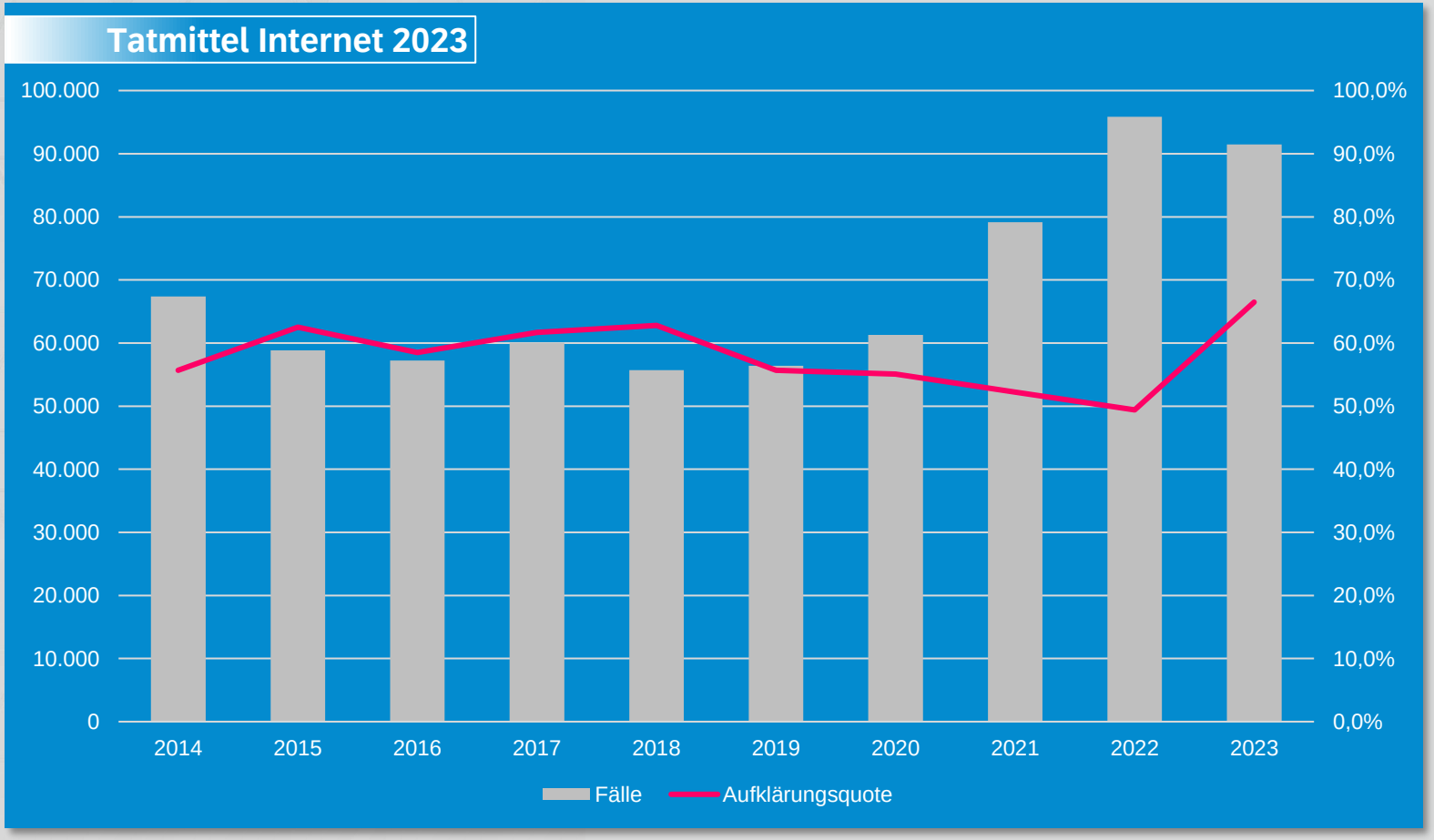


Cybercrime im weiteren Sinn
Straftaten, bei denen das Internet zur Tatbestandsverwirklichung verwendet wird.



Zahlen Cyberkriminalität

Cyberkriminalität 2023



POLIZEI Nordrhein-Westfalen Dortmund

Formen von Cybercrime

Formen von Cybercrime

- **Sexualisierte Gewalt:** Cybergrooming; Sexting
- **Handygewalt**
- **Digitale Erpressung:** Ransomware, Sextortion
- **Schadsoftware / Malware:** Viren; Trojaner
- **Gewaltkriminalität:** Cybermobbing; Cyberstalking
- **Eigentumsdelikte:** Phishing; Identitätsdiebstahl; Fakeshops
- **DDoS-Angriffe / Botnetze**
- **Social Engineering**
- **CEO Fraud** (Chef Betrug)
- **Angriff auf das „Internet der Dinge“** (IoT)
- **Cybercrime-as-a-Service**


Cybergrooming
Quelle: Adobe Stock/Polizei NRW

Sexualisierte Gewalt

Cybergrooming

Cybergrooming ist die gezielte Anbahnung sexueller Kontakte mit Minderjährigen über das Internet.

- Täter geben sich als gleichaltrig aus
- Sie wollen das Vertrauen der Minderjährigen gewinnen
- Überreden ihre Opfer, ihnen freizügige Selbstportraits zu schicken => Druckmittel => Erpressung zwecks weiterer Handlungen
- Ziel: Treffen in realer Welt zwecks Missbrauch oder Gelderpressung

Sexualisierte Gewalt

Beispiel für Cybergrooming

- Viele junge Mädchen nutzen Plattformen wie „Moviestar Planet“
- Kriminelle geben sich als gleichaltrig aus und laden die Mädchen über den kostenlosen Chat nach Snapchat ein
- Hier werden die Betroffenen direkt nach freizügigen Bildern/Nacktbildern gefragt

Quelle: www.moviestarplanet2.com

An alle Eltern 15. Jan.

★☆☆☆☆

Liebe Eltern, passt bitte auf was die Leute da schreiben , es sind da einige die machen richtige sexuelle Belästigungen, also wenn da noch 10-15 jährige oder noch jünger dabei sind, finde ich schon heftig was da geschrieben wird

Achtung! Brut-Herd für Pädophile!!! Vor 1 J.

★☆☆☆☆

Meine Tochter wollte diese App unbedingt, um coole Videos zur erstellen. Keine Frage, dafür ist die App super geeignet.
Zur Probe haben wir diese App auf unserem IPad installiert und erstmal eine fiktive Mailadresse zum Test angegeben. Es dauerte nicht lange, bis die ersten sehr eindeutigen Anfragen kamen. Unsere Tochter war so geschockt v Mehr

Vorsicht !!! Vor 3 J.

★☆☆☆☆

...Passt auf eure Kinder auf, dieses Spiel ist nichts anderes als ein Tummelplatz für Pädophile. Spiel wurde erfolgreich gelöscht und bleibt es auch☠☠☠

Sexualisierte Gewalt

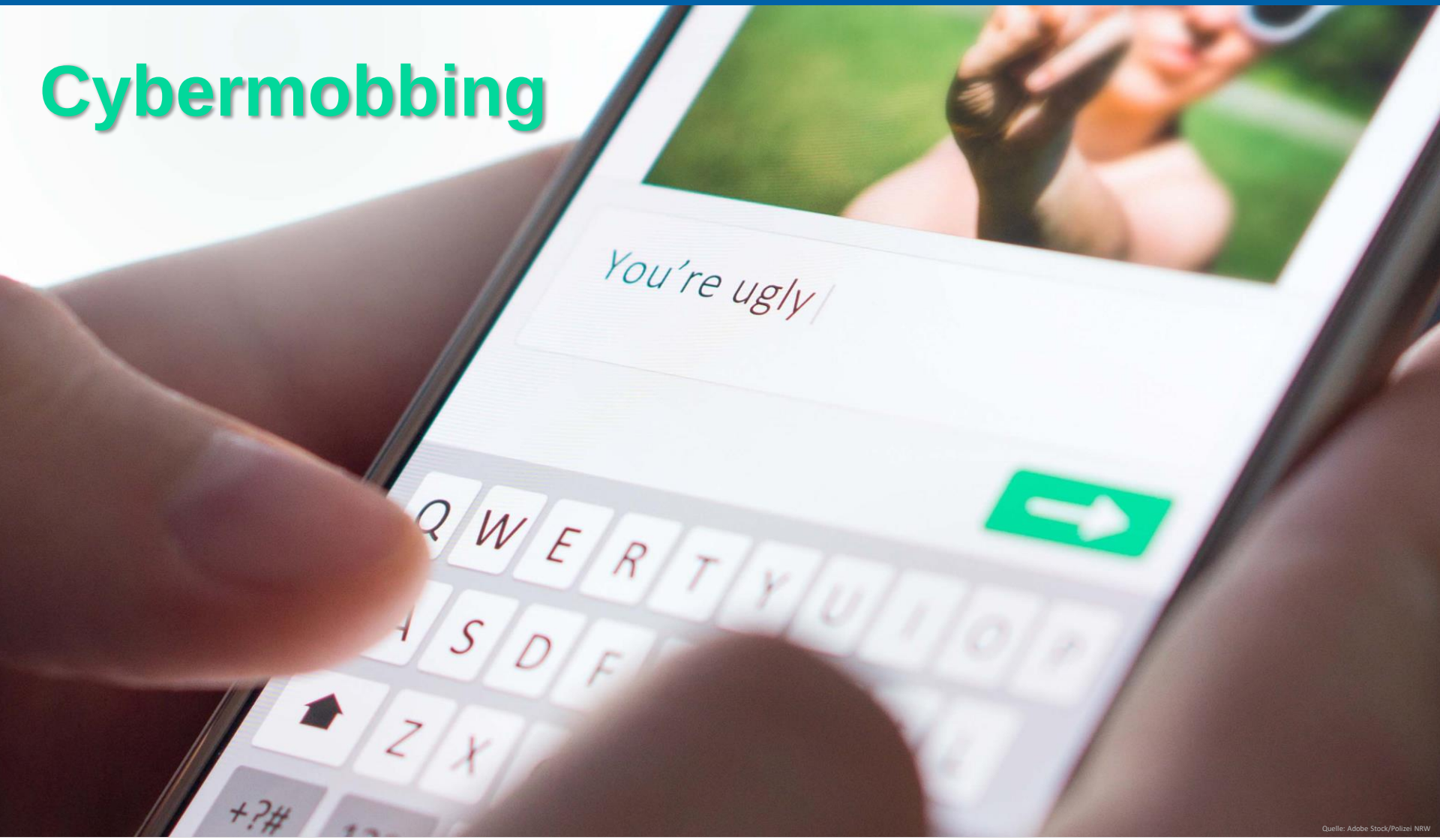
- Anbahnung von sexueller Gewalt gegen Minderjährige
- Kontakt über TikTok, Instagram, Facebook, Fortnite, YouTube, Twitch, Kleinanzeigen, …
- Gespräch wird in private Chats verlagert
- Gespräch wird auf Sexualität bzw. bisherige sexuelle Erfahrungen gelenkt
- Geldgeschenke oder andere „Vorteile“ werden angeboten
- Zuschicken von Bildern oder Videos wird verlangt, Webcam soll genutzt werden
- reales Treffen wird ggf. angestrebt

JA!

Man kann mit 12-jährigen Kindern über Pornographie reden!

Sonst tut es ein Anderer!

Cybermobbing



Gewaltkriminalität

Cybermobbing ist die Nutzung digitaler Endgeräte und Internet durch Personen oder Gruppen zum absichtlichen und systematischen Belästigen, Bedrohen, Bloßstellen und Ausgrenzen anderer Personen über einen längeren Zeitraum!

Fortsetzung oder Ergänzung “klassischer“ Mobbinghandlungen über Chats, WhatsApp, Instagram, TikTok, Facebook, YouTube, Blogs, Foren etc.

Gewaltkriminalität

Cybermobbing - Besonderheiten gegenüber „klassischem“ Mobbing:

- **Permanente Belästigung** mittels mehrerer Medien (Smartphone, Social Media,…)
- Es kommt zu **wiederholten Vorfällen**
- **Sehr schnelle, intensive Verbreitung** an sehr großen Personenkreis
- **Inhalte** lassen sich nur schwer oder überhaupt **nicht mehr löschen**
- **Anonymer Täterkreis** oder das Handeln unter **falscher Identität**; daher ist die Hemmschwelle erheblich niedriger
- Eingriff in das Privatleben - Opfer haben **kaum noch „Rückzugsraum“**
- Schikanierendes Verhalten **systematisch über längeren Zeitraum**

Gewaltkriminalität

Cybermobbing - in Frage kommende Straftaten:

- **Beleidigung** - §185 StGB
  (vorsätzliche Kundgabe der Missachtung/Nichtachtung der Ehre eines Anderen)
  [Freiheitsstrafe bis zu einem Jahr oder Geldstrafe]

- **Üble Nachrede** - §186 StGB
  (Dinge über Menschen behaupten oder verbreiten, die andere herabwürdigen oder verächtlich machen; auch Dinge „weitersagen“, von denen man selbst glaubt, dass sie wahr sind *[Freiheitsstrafe bis zu einem Jahr oder Geldstrafe]*

- **Verleumdung** - §187 StGB
  (das bewusste behaupten oder verbreiten falscher Tatsachen über andere Menschen)
  [Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe]

- Nur ein Auszug vieler möglicher Straftatbestände! -

Gewaltkriminalität

Cyberstalking

Das fortwährende Belästigen und Verfolgen/Nachstellen im virtuellen Raum, gegen den Willen einer anderen Person.

Hierzu zählen auch sexuelle Belästigungen.

Das Nachstellen und das „Aussuchen“ eines Opfers geschieht grundsätzlich im virtuellen Raum.

Technische Beispiele: GPS-Wanzen, Ortungs-Apps & Plattformen

Gewaltkriminalität

Cyberstalking

- Nachstellung - §238 StGB [Freiheitsstrafe bis zu drei Jahren oder Geldstrafe]

Strafbar macht sich, wer einen Menschen unbefugt nachstellt, indem er beharrlich

1. seine räumliche Nähe aufsucht,
2. unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte Kontakt zu ihm herzustellen versucht,
3. unter missbräuchlicher Verwendung von dessen personenbezogenen Daten Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte veranlasst, mit diesem Kontakt aufzunehmen,
4. ihn mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit, oder Freiheit seiner selbst oder einer ihm nahe stehenden Person bedroht oder
5. eine andere vergleichbare Handlung vornimmt und dadurch seine Lebensgestaltung schwerwiegend beeinträchtigt.

POLIZEI Nordrhein-Westfalen Dortmund

Grundschutz & Internetsicherheit

Ausgangslage

Nutzung von Smartphones, Laptops, Tablets, Smart Watches, IoT

- Kommunikation mit Freunden/Familie
- Nutzung sozialer Netzwerke & Partnerbörsen
- Online-Shopping & E-Commerce
- Musik-, Video- & Gaming-Plattformen
- Online Banking
- Bildung & Nachrichten

Relevanz des Smartphones

- Zeichen des Erwachsenwerdens und der Gruppenzugehörigkeit
- personalisiertes Zubehör, modischer Begleiter, Statussymbol
- Ausdruck der eigenen Identität
- wichtigste Mittel der Kommunikation im Freundeskreis

Top 5 Apps 2024

Wichtigste Apps Top 5

	12-13 Jahre	14-15 Jahre	16-17 Jahre	18-19 Jahre
Rang 1	WhatsApp (81 %)	WhatsApp (77 %)	WhatsApp (81 %)	WhatsApp (86 %)
Rang 2	YouTube (35 %)	TikTok (31 %)	Instagram (37 %)	Instagram (45 %)
Rang 3	TikTok (21 %)	Instagram + Snapchat (jew. 29 %)	TikTok (25 %)	YouTube + TikTok (jew. 24 %)
Rang 4	Snapchat (16 %)	YouTube (22 %)	YouTube (22 %)	Spotify (17 %)
Rang 5	Instagram (11 %)	Spotify (12 %)	Snapchat (21 %)	Snapchat (15 %)

Quelle: JIM 2024, Angaben in Prozent, Basis: Befragte, die ein Handy/Smartphone besitzen, n=1.122

Kinder und Jugendliche sind vernetzt - OHNE ihre Eltern!

Xhamster

Pinterest

Kleinanzeigen

Instagram

Facebook

Youporn

Snapchat

Steam

Twitch

TikTok

Knuddels.de

Discord

Chatroulette

Call of Duty

Fortnite

YouTube

Minecraft

Soziale Netzwerke & Apps

Quelle: www.kaufda.de/info/apps-in-echtzeit

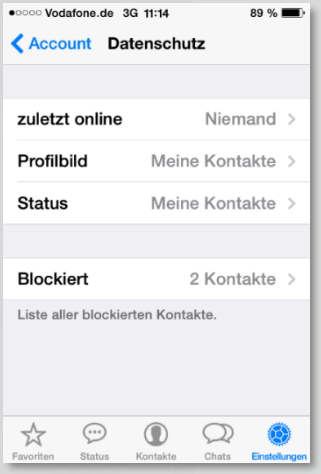
Soziale Netzwerke & Apps

Privatsphäre schützen

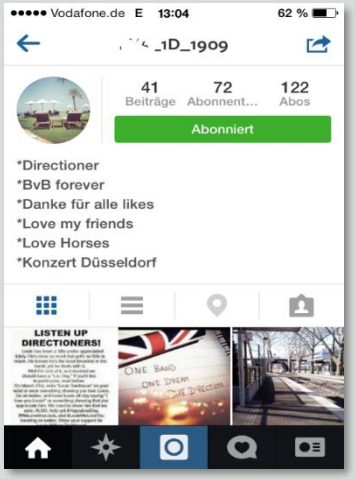
Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben.

=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!

[Profilbild, pers. bezogene Daten, Freunde-Einstellungen, öffentliche Daten, Selfies, Likes]



WhatsApp
Datenschutzeinstellungen

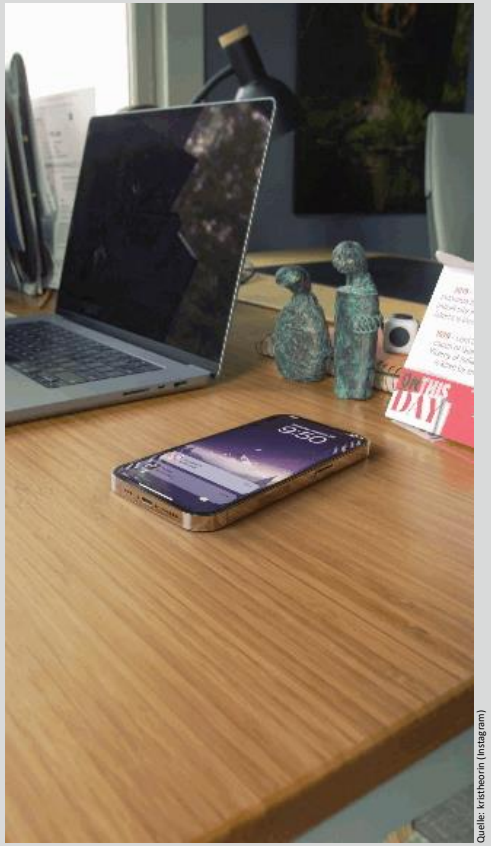


Instagram
Profilinformationen

Soziale Netzwerke & Apps

Foto- und Smartphone Empfehlungen:

- So wenig Fotos wie möglich veröffentlichen/verschicken
- Niemals „private“ Bilder verschicken - auch nicht an „beste“ Freunde
- Dienste wie z.B. Snapchat bieten keine Sicherheit
- Keine Bilder mit Wiedererkennungswert als Profilbild
- Fakten prüfen und hinterfragen
- Geräte immer gegen unbefugten Zugriff schützen
- Einstellungen/Einschränkungen altersgerecht vornehmen
- Schutzsoftware installieren (gegen Schadprogramme, Ortung & Fernlöschung im Verlustfall)
- In-App-Käufe/App-Downloads deaktivieren oder sperren
- Smartphone zulegen, wenn ein verantwortungsbewusster Umgang bzw. das Begreifen der Funktionen möglich sind



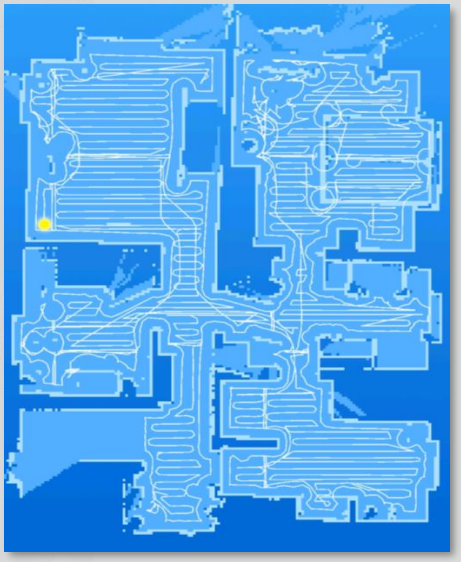
Quelle: kristhecrin (Instagram)

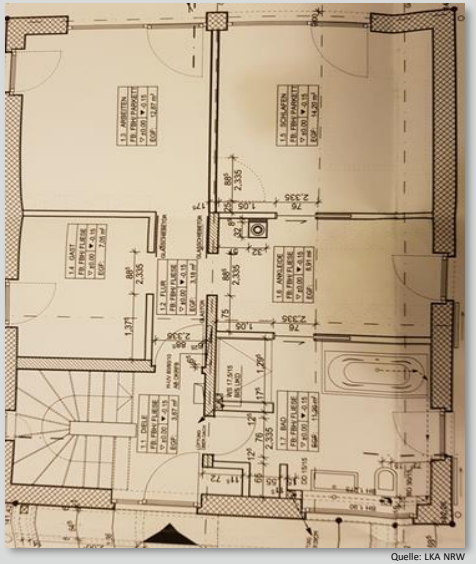
Internet of Things

Der Begriff „Internet of Things“ (IoT) oder auch das „Internet der Dinge“ steht für eine vernetzte Welt aus smarten Geräten, Sensoren und weiteren Technologien.

Beispiele für IoT: **Smart Home**, **Smart Toys**, **Wearables**, **Digitale Assistenten**, **Smart-TV**, **Smart City**

Internet of Things



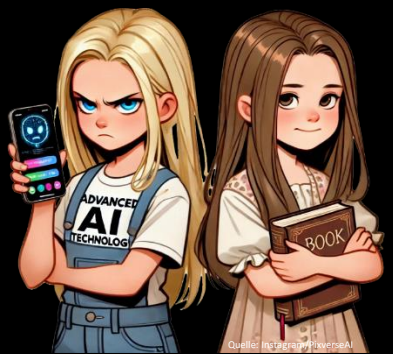


Quelle: LKA NRW

Künstliche Intelligenz

Künstliche Intelligenz


runway


ADVANCED
AI
TECHNOLOGY
BOOK


runway

Fotos & Videos

Das Fotografieren innerhalb eines Gebäudes/Schulgelände kann durch den Inhaber des Hausrechts grundsätzlich untersagt oder eingeschränkt werden.

Der Gebrauch von Smartphones oder anderen elektronischen Geräten (Smartwatches, Tablets etc.) sollte klar geregelt sein!

Zum Beispiel:

- → **Handyordnung**
- → **Devices einsammeln** (NUR wenn dies für die Aufrechterhaltung des Schulbetriebs erforderlich ist)
  - → Lehrkräfte dürfen Devices nicht „vorsorglich“ einkassieren
- → **Kinder-/Jugendpornografische Inhalte** müssen unmittelbar bei der Polizei anzeigt werden

Das Zugänglichmachen von Gewalt- und Pornovideos für unter 18 Jährige ist eine Straftat!

Dazu gehört auch das Verschicken auf andere Handys!

Beispiele für strafbares Handeln

- Unter den Rock fotografiert und weiter verbreitet
- Lehrer während des Unterrichts gefilmt
- Mitschüler verprügelt und gefilmt
- Heimliche Filmaufnahmen in der Umkleidekabine
- Verbreiten von Gewaltvideos unter Schülern
- **Handygewalt** ist eine Form digitaler Gewalt, bei der das Opfer gezielt herabgesetzt, erpresst, bedroht oder tätlich angegriffen wird

- Verfassungsfeindliche Symbole
- Extremismus
- Rassistische Inhalte

- Gewaltdarstellungen
- Tierquälerei
- Folter

- Pornografie 18+
- Missbrauchsabbildungen
- Verletzung Persönlichkeitsrechte

Persönlichkeitsrechte

- **Fotografieren oder Filmen anderer Personen**
- **Veröffentlichen von Bildern oder Videos**
- **Weitergabe von Bildern oder Videos**

Das Recht am eigenen Bild

Fotografierte Personen haben das Recht, eine Aufnahme zu untersagen!

Laut Bundesdatenschutzgesetz ist ein Digitalfoto eine „Erhebung personenbezogener Daten“, die nur mit Zustimmung der Betroffenen erfolgen darf. Der Verstoß ist eine Ordnungswidrigkeit!
(§ 4 i.V. m. § 43 BDSG)

„Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder zur Schau gestellt werden“ (§22 KunstUrhG)

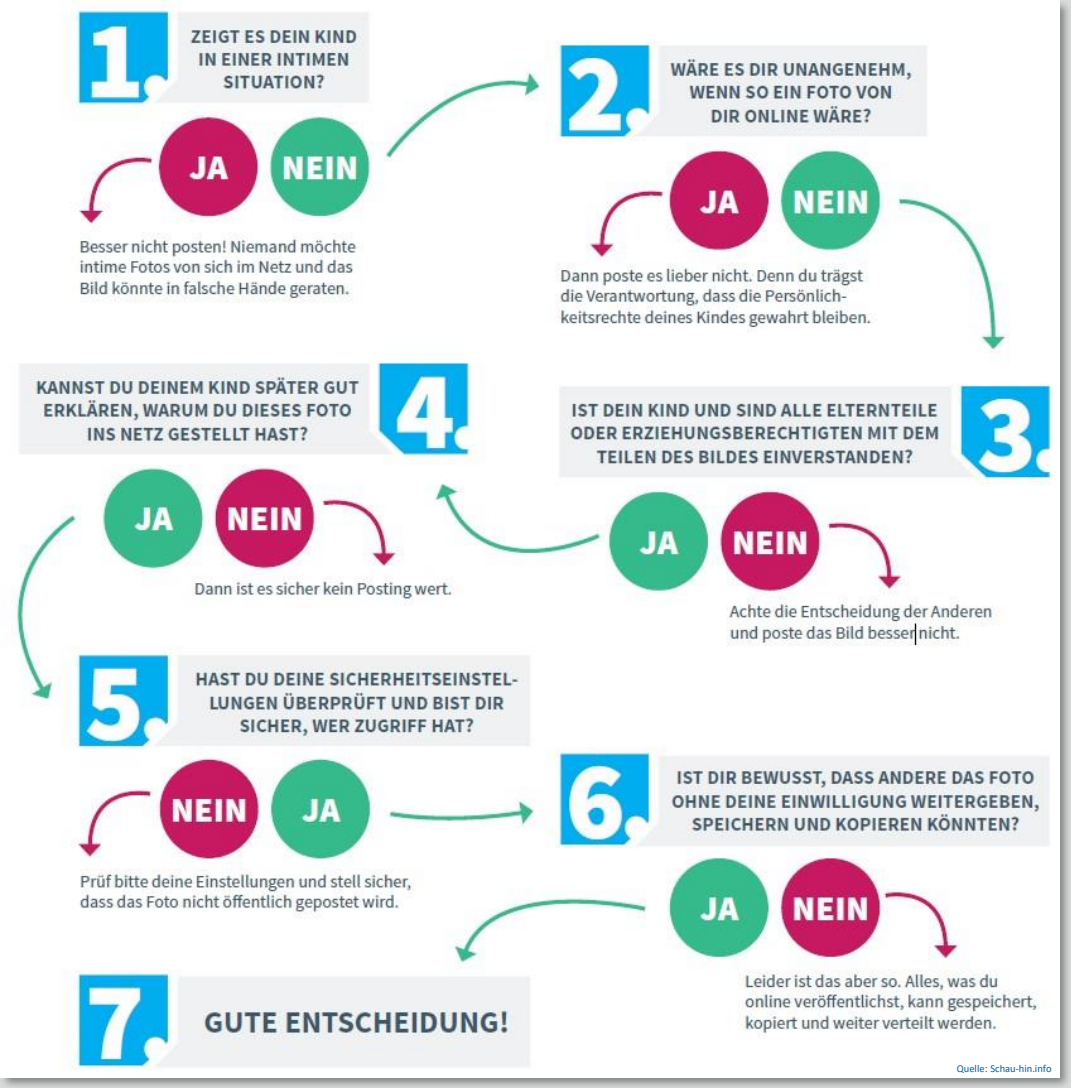
!! Veröffentlichen ohne Einwilligung ist eine Straftat !!

Persönlichkeitsrechte

Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§201a StGB):

(1) Mit Freiheitsstrafe oder mit Geldstrafe wird bestraft, wer

1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
2. eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
3. eine durch eine Tat nach den Nummern 1 und 2 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht.


1.
ZEIGT ES DEIN KIND IN EINER INTIMEN SITUATION?
JA
NEIN
Besser nicht posten! Niemand möchte intime Fotos von sich im Netz und das Bild könnte in falsche Hände geraten.
2.
WÄRE ES DIR UNANGENEHM, WENN SO EIN FOTO VON DIR ONLINE WÄRE?
JA
NEIN
Dann poste es lieber nicht. Denn du trägst die Verantwortung, dass die Persönlich-keitsrechte deines Kindes gewahrt bleiben.
3.
IST DEIN KIND UND SIND ALLE ELTERNTEILE ODER ERZIEHUNGSBERECHTIGTEN MIT DEM TEILEN DES BILDES EINVERSTANDEN?
JA
NEIN
Achte die Entscheidung der Anderen und poste das Bild besser nicht.
4.
KANNST DU DEINEM KIND SPÄTER GUT ERKLÄREN, WARUM DU DIESES FOTO INS NETZ GESTELLT HAST?
JA
NEIN
Dann ist es sicher kein Posting wert.
5.
HAST DU DEINE SICHERHEITSEINSTEL-LUNGEN ÜBERPRÜFT UND BIST DIR SICHER, WER ZUGRIFF HAT?
NEIN
JA
Prüf bitte deine Einstellungen und stell sicher, dass das Foto nicht öffentlich gepostet wird.
6.
IST DIR BEWUSST, DASS ANDERE DAS FOTO OHNE DEINE EINWILLIGUNG WEITERGEBEN, SPEICHERN UND KOPIEREN KÖNNTEN?
JA
NEIN
Leider ist das aber so. Alles, was du online veröffentlichst, kann gespeichert, kopiert und weiter verteilt werden.
7.
GUTE ENTSCHEIDUNG!
Quelle: Schau-hin.info

Kettenbriefe & Suizid

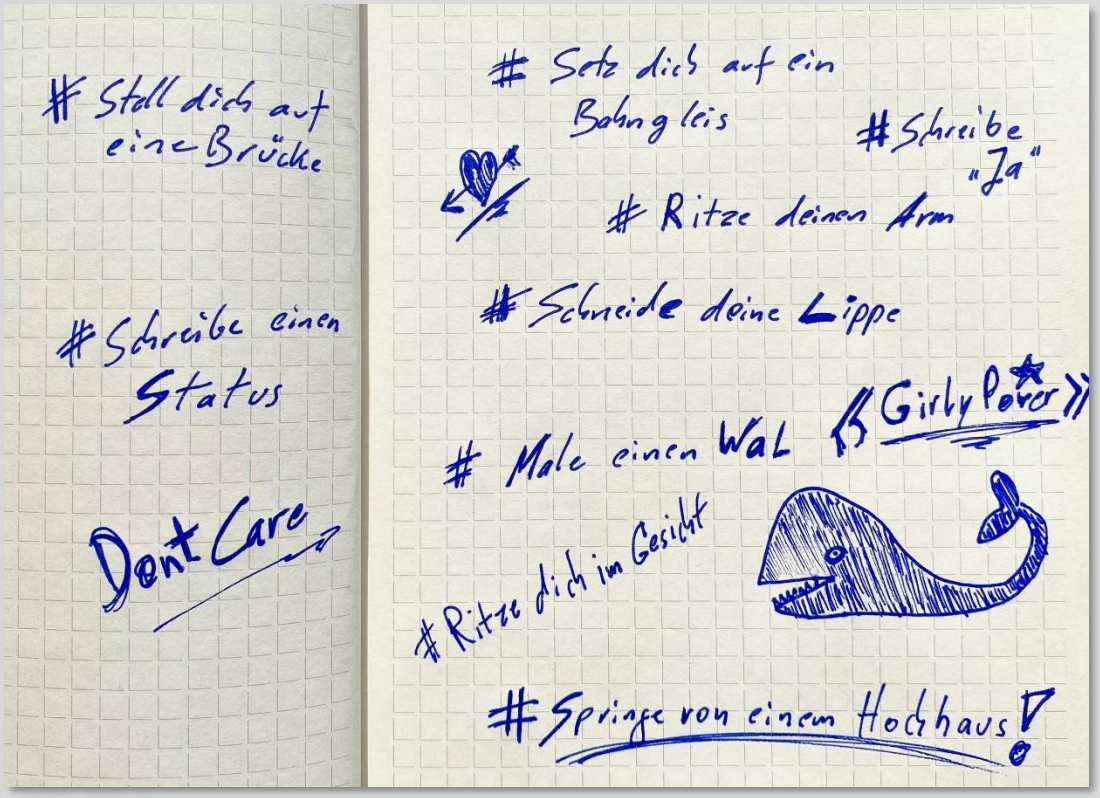
Kettenbriefe

- Sprachnachrichten
- Pornografische Inhalte
- Rechte Inhalte

=> keine Kettenbriefe weiterleiten!!

(Suizid)-Challenges

- Blue Whale Challenge
- Blackout Challenge
- Salt Challenge
- Hot Water Challenge
- Tide Pod Challenge
- Hot Chip Challenge



POLIZEI Nordrhein-Westfalen Dortmund

Schutz & Prävention

Schutz & Prävention

Passwortschutz

Cybercrime-Präventionskampagne des LKA NRW:

„MACH DEIN PASSWORT STARK!“

- Mindestens 12 Zeichen aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen
- Keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch
- Für verschiedene Onlinezugänge unterschiedliche Nutzernamen/Passwörter nutzen
- Keine plattformübergreifenden Passwörter verwenden
- Passwörter nur an geeigneten Stellen und vor Dritten geschützt aufbewahren
- Keine bereits benutzen Passwörter wiederverwenden
- „Passwort merken“-Funktion von Anwendungen im Browser/Apps vermeiden

Passwortschutz

Wie erstellt man ein starkes Passwort?

Sie verwenden zum Beispiel einen Satz, den Sie sich gut merken können und verwenden die jeweils ersten Zeichen:

Ich hab Bock auf 2 Döner & 3 Pommes Rot-Weiß!

IhBa2D&3PR-W!

Zusammenfassung

- Starke Passwörter verwenden
- Privatsphäre schützen – sparsam sein, mit der Weitergabe von persönlichen Daten
- Misstrauisch sein (E-Mails; Kontaktanfragen,…)
- Fragwürdige Mails löschen -> keine Anhänge öffnen
- Endgeräte sichern (PIN, Face-ID, Passwort, Virenprogramm, Firewall, VPN)
- Authentifizierungsverfahren nutzen (Zwei-Faktor-Authentisierung, Smart Card, Biometrisches Profil)
- Betriebssysteme, Browser, Software regelmäßig updaten
- PC/Tablet-Mitbenutzerrechte einschränken
- Sicherheitszertifikate prüfen bei Websites
- Achtung bei Software Downloads
- APPs prüfen (IOS/Android)
- Smartphones einschränken - PIN (Standard-Apps blockieren / In-App-Käufe blocken / …)
- Kindersicherung/Jugendschutzeinstellungen verwenden (Apple, Android, Xbox, Playstation)
- Daten sichern (USB-Stick, externer Datenträger, Cloud)
- WLAN absichern/verschlüsseln (WPA2 – Wi-Fi Protected Access)
- Hardware vor Diebstahl/Spionage schützen (Sichtschutz für Laptop, RFID Blocker)

Nützliche Informationen

www.polizei-beratung.de

www.polizeifürdich.de

www.schau-hin.info

www.klicksafe.de

www.medien-kindersicher.de

www.jugendschutz.net

www.mach-dein-passwort-stark.de

www.flimmo.de

www.medienanstalt-nrw.de

www.bsi-fuer-buerger.de

www.cyberfibel.de

www.hateaid.org

Tipps für Eltern & Lehrer

- Machen Sie sich mit den Funktionen von PC- und Mobile Devices vertraut sowie deren Internetfähigkeit
- Achten Sie auf entsprechende Vorkommnisse in der Schule oder Jugendfreizeiteinrichtung
- Sensibilisierung der Kinder/Jugendlichen über Auswirkungen und Folgen der Handy-Nutzung und daraus resultierender, möglicher Straftatbestände
- Informieren Sie die Polizei, wenn der Verdacht einer Straftat vorliegt

Mach dein Handy nicht zur Waffe

Nachricht von Ella

POLIZEI Nordrhein-Westfalen Dortmund

Was können Sie tun, wenn Sie Opfer geworden sind?

- Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen
- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial - wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos u. v. m. - sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Wenn Sie technisch versiert sind, können Sie diese Beweismittel auch abspeichern, ausdrucken oder z. B. via Screenshots sichern. Ist Ihnen dies nicht möglich, weil Sie der gesamte Tathergang zu sehr belastet, bitten Sie eine Person Ihres Vertrauens, diese Beweise für Sie zu sichern.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.
- Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht unmittelbar auf spezialisierte Cybercrime-Experten treffen und deshalb in den meisten Fällen noch an eine spezialisierte Fachdienststelle weitergeleitet werden oder von dort Rückfragen erhalten.

POLIZEI Nordrhein-Westfalen Dortmund

Hilfsangebote

- Wenn Sie Opfer von Cybercrime geworden sind, stehen Ihnen die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.
- Auch die Folgen einer Tat können identisch sein. Je nachdem kann finanzieller Schaden oder eine psychische Belastung oder sogar beides ihr zukünftiges Leben grundlegend verändern.
- Scheuen Sie sich daher nicht, professionelle Hilfe zur Bewältigung des Erlebten zu suchen.
- Ein erster Schritt kann ein Anruf bei einer Hilfsorganisation, einem gemeinnützigen Verein zur Unterstützung von Kriminalitätsopfern (z.B. WEISSER RING) oder einer anderen Hilfeeinrichtung in Ihrer Stadt sein; z.B. die Telefonseelsorge unter 0800 111 0111 oder unter 0800 111 0222. Eine kostenlose und anonyme Beratung in vielen Sprachen bietet das „Hilfetelefon Gewalt gegen Frauen“ unter der Nummer 08000 116 016 an.
- Kinder- und Jugendtelefon 0800 111 0333 Nummer gegen Kummer, anonym und kostenlos erreichbar montags – samstags 14.00 - 20.00 Uhr
- Weiterhin kann es wichtig sein, sich über Verbraucherrechte und Regelungen für den Online-Warenhandel zu informieren. Falls in Ihrem Fall ein Rücktrittsrecht besteht, machen Sie davon Gebrauch, solange die Fristen nicht verstrichen sind.

Vielen Dank für Ihre Aufmerksamkeit

Kriminalprävention Cybercrime
Marcel Wessollek

Tel.: 0231-132 7053
E-Mail: marcel.wessollek@polizei.nrw.de