Quelle: Adobe Stock/Polizei NRW

Kriminalprävention Cybercrime

Prävention von Computer- & Internetkriminalität

Themen & Inhalte

- Definition Cybercrime
- Formen von Cybercrime
- Gefahren im Internet
- Schutz & Prävention

Definition Cybercrime

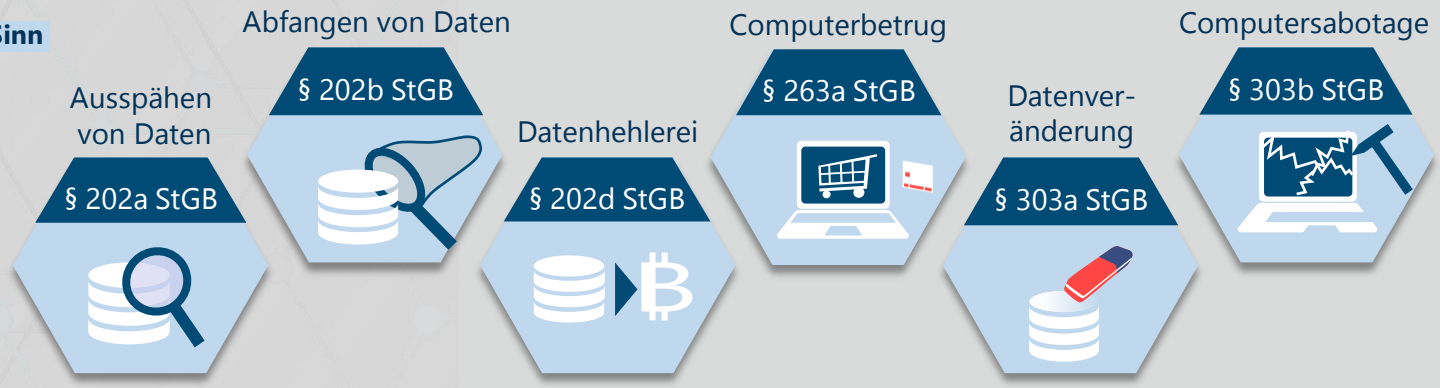
Definition Cybercrime

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.

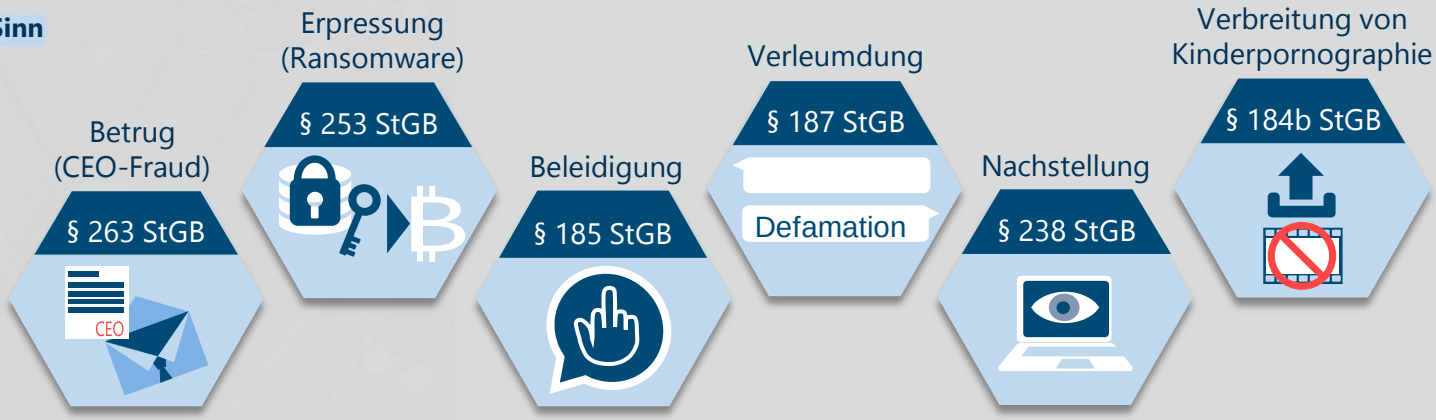
// Straftaten richten sich dabei grundsätzlich gegen das Vermögen oder die persönliche Integrität; am häufigsten unter Verwendung des Tatmittels Internet und E-Mail

Definition Cybercrime

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



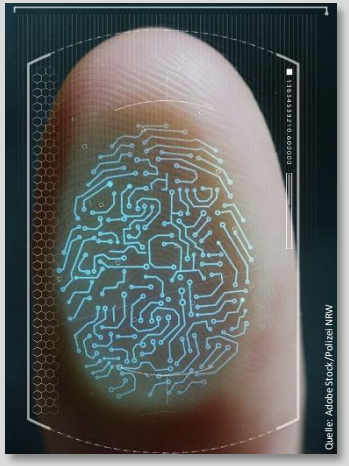
Cybercrime im weiteren Sinn
Straftaten, bei denen das Internet zur Tatbestandsverwirklichung verwendet wird.



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**



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.


PHISHING
USER NAME
PASSWORD

Phishing

Phishing

Unter dem Begriff „**Phishing**“ versteht man den Versuch, durch gefälschte E-Mails/SMS (mit Schadcode im Anhang oder Link zu einer präparierten Website), gefälschte Webseiten, Kurznachrichten oder Videolinks an die persönlichen Daten eines Internetnutzers zu gelangen und so einen Identitätsdiebstahl zu begehen.

Die Täter verwenden hier gefälschte, täuschend echt aussehende E-Mails und Links zu Websites von namenhaften Marken, Unternehmen, Händlern oder Banken um die Opfer zu ködern.
Geben die Betroffenen dann ihre persönlichen Daten, Passwörter etc. in die fingierten Eingabemasken ein, schicken sie diese dann unbewusst an die Cyberkriminellen.

Phishing

Schutz vor Phishing

- Keine persönlichen und beruflichen Informationen in sozialen Netzwerken
- Starke und komplexe Passwörter verwenden
- Seien Sie misstrauisch (E-Mails; Kontaktanfragen,…)
- Identität und Berechtigung des Ansprechenden sicherstellen
- Fragwürdige Mails löschen -> keine Anhänge öffnen
- Keine (sensiblen) Informationen an Unbekannte weitergeben
- Authentifizierungsverfahren nutzen; z.B. Zwei-Faktor-Authentisierung
- Beenden Sie eine Online-Session immer über den regulären Log-out
- Geben Sie niemals persönliche Daten auf unverschlüsselten Seiten ein
- Antivirus und Firewall Systeme sollten immer eingeschaltet und aktuell sein

Fakeshops

Quelle: Adobe Stock/Polizei NRW

Fakeshops sind gefälschte Internet-Verkaufsplattformen, die auf den ersten Blick nicht als solche zu erkennen sind.

Sie sind teilweise Kopien real existierender Websites und wirken daher seriös und lassen beim Käufer selten Zweifel an ihrer Echtheit aufkommen.

Wesentliche Merkmale von Fakeshops:

- Ungewöhnlich günstige Preise für Markenartikel
- Das Impressum des Onlineshops fehlt, ist unvollständig oder Inhalte sind nicht korrekt dargestellt
- Die Ware kann nur gegen Vorkasse bezahlt werden
- Gütesiegel wurden nur als Bild auf die Seite eingebunden
- Die Allgemeinen Geschäftsbedingungen sind fehlerhaft/unvollständig oder fehlen
- Der Domainname ergibt keinen logischen Sinn
- Die Ware ist „immer“ verfügbar

Wie kann man sich vor Fakeshops schützen:

- Wenn sie unsicher sind, nehmen Sie Kontakt mit dem Shop Betreiber auf
- Recherchieren sie im Internet nach dem Shop (Firmenadresse, Bewertungen)
- Gütesiegel des Shops per Mausklick überprüfen
- Nutzen Sie nur ihnen bekannte Bezahldienste oder den Kauf auf Rechnung
- Seien Sie misstrauisch, wenn die Kommunikation nur über E-Mail erfolgen kann
- Kontrollieren Sie den Domain-Namen des Onlineshops
- Folgen Sie keinen Links aus Spam-Mails zu den Seiten des angebotenen Shops
- Vermeiden Sie Käufe und Überweisungen außerhalb der Geschäftszeiten ihrer Bank um im Notfall einen Ansprechpartner zu haben
- Eingebundene Links des Onlineshops zu Social Media-Kanälen prüfen
- Handelsregisternummern prüfen www.handelsregister.de / Prüfung der Umsatzsteuer-ID https://ust-id-pruefen.de

Quelle: Adobe Stock/Polizei NRW

Deep Fakes

Das Wort „**Deep Fake**" ist eine Wortkombination aus "Deep Learning„ (Methode des maschinellen Lernens resp. künstlicher Intelligenz) und "Fakes" (Fälschung, Imitation). Ein Deep Fake ist also ein Bild, Video oder Audioinhalt, der mithilfe Künstlicher Intelligenz gefälscht bzw. verändert wurde!

Mittels Deep-Learning-Technologie lassen sich mittlerweile Fotos und Videos so bearbeiten, dass oft keine Hinweise mehr erkennbar sind, ob diese echt sind oder manipuliert wurden.

Es gibt verschiedene Arten von Deep Fakes, welche allein oder in Kombination auftreten können:

- **Face Swapping**
- **Voice Deep Fake**
- **Body Puppetry**

Deep Fakes

Beim **Face Swapping** werden Gesichter auf Bildern oder Videos durch künstlich erzeugte Gesichter anderer Personen ersetzt. Dabei wird die Mimik (Mund-, Kinn- und Augenbewegungen) komplett auf das neu erzeugte Gesicht übertragen.

Bei einem **Voice Deep Fake** wird häufig eine echte Stimme mittels KI nachgeahmt. Mittels künstlicher Intelligenz werden überzeugende Sprachansätze erstellt, die so klingen sollen, als ob eine bestimmte Person diese sagt.

Von **Body Puppetry** ist die Rede, wenn einzelne Bewegungen oder komplette Bewegungsabläufe einer Person auf eine andere Person übertragen werden.

Deep Fakes

Deep Fakes können auch negative und strafrechtlich relevante Folgen nach sich ziehen, wenn sie eine Bedrohung für Wirtschaft, Gesellschaft oder Demokratie darstellen.

Besonders folgende Anwendungsbereiche sind typisch für Deep Fakes:

- **Fake News** (gezielte Desinformation)
- **Propaganda**
- **Social Engineering**
- **CEO Fraud**
- **Diskreditierung von Einzelpersonen & Erpressung**
- **Verletzung der Persönlichkeitsrechte**
- **Waren- und Kreditbetrug**
  - Voice-ID-Systeme (Stimmidentifizierung bei Bank, Versicherung ---> Stimme als Passwort)
  - ID-Provider (digitale Identität zwecks Kontoeröffnung ---> Geldwäsche)
  - Kriminalistik (Fälschung von Beweismittel, Verschleierung von Straftaten)

Deep Fakes

Schutz vor Deep Fakes

- Sicherstellen, dass Mitarbeiter & Familie die Gefahren von Deep Fakes kennen
- Das Erkennen von Deep Fakes schulen
- Medienkompetenz aufbauen und hochwertige Nachrichtenquellen nutzen
- Misstrauisch sein - (Sprach-)Nachrichten, Anrufe und Videos hinterfragen
- Quellen und Herkunft der Daten prüfen
- Keine persönlichen und beruflichen Informationen in sozialen Netzwerken
- Keine (sensiblen) Informationen an Unbekannte weitergeben
- Deep Fake-Erkennungssoftware/Tools verwenden (Anti-Fake-Technologie)
    - Kryptografischer Algorithmus mit Hashfunktion
    - Künstliche Intelligenz & Digitaler Fingerabdruck mit Blockchain Technologie
    - Tools zur Analyse der Mundpartie und Augenreflexion
    - FaceForensic Technologien

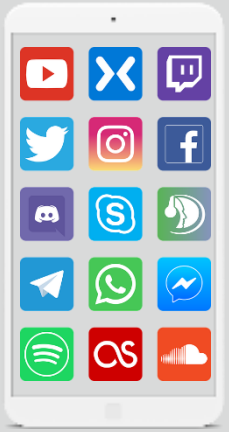
POLIZEI
Nordrhein-Westfalen
Dortmund

Gefahren im Internet

Ausgangslage

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

- Kommunikation mit Freunden/Familie
- Nutzung sozialer Netzwerke & Partnerbörsen
  - Bilder und Videos erstellen, verschicken, teilen
- Online-Shopping & E-Commerce
- Nutzung von Musik-, Video- & Gaming-Plattformen
- Bankgeschäfte
- Nachrichten lesen & Themen recherchieren



Relevanz des Smartphones

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

Soziale Netzwerke & Apps

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

Soziale Netzwerke & Apps

Foto- und Smartphone Empfehlungen:

- So wenig private Informationen wie möglich veröffentlichen/verschicken!
- Niemals „private“ Bilder verschicken - auch nicht an „beste“ Freunde
- Vermeintlich sichere Dienste wie z.B. Snapchat bieten keine Sicherheit
- Keine Bilder mit Wiedererkennungswert als Profilbilder verwenden
- Geräte immer gegen unbefugten Zugriff schützen (PIN; Passwort; Face-ID)
- Einstellungen und Einschränkungen altersgerecht vornehmen
- Schutzsoftware installieren (gegen Schadprogramme, Ortung & Fernlöschung im Verlustfall)
- In-App-Käufe oder App-Downloads unbedingt mit Passwort schützen bzw. sperren

Quelle: www.klicksafe.de

Internet of Things

IoT-Angriffe

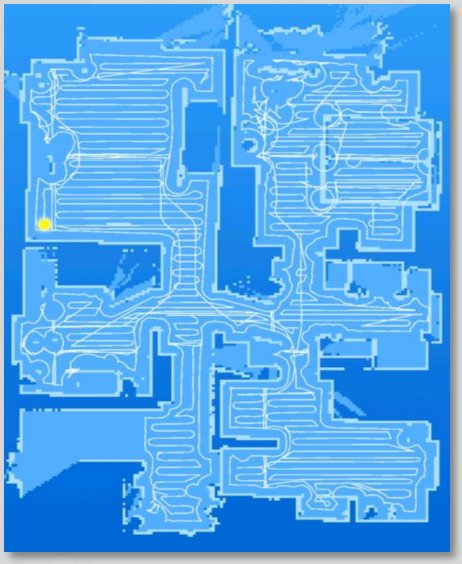
Der Begriff „Internet of Things“ (IoT) oder auch das „Internet der Dinge“ steht für eine vernetzte Welt aus smarten Geräten, Sensoren und weiteren Technologien.

<u>Beispiele für Internet of Things:</u>

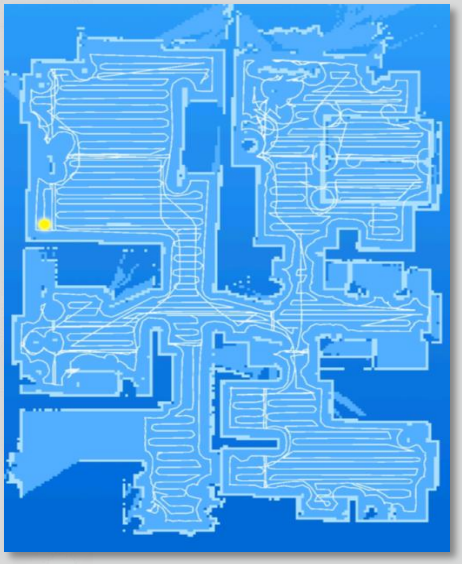
- **Smart Home**
- **Smart Toys**
- **Wearables**
- **Digitale Assistenten**
- **Smart-TV**
- **Smart City**

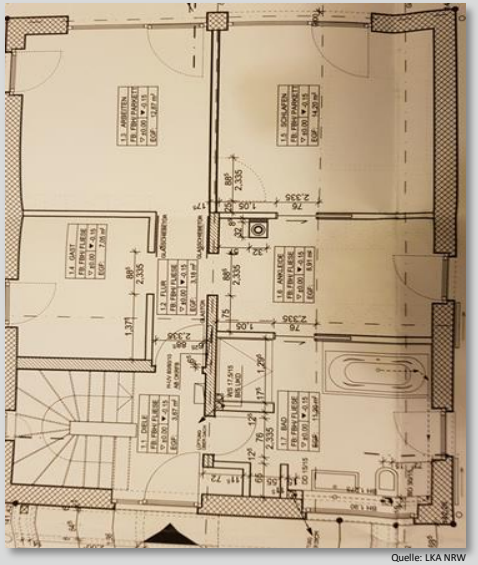
Internet of Things

Internet of Things



Internet of Things





Quelle: LKA NRW

Persönlichkeitsrechte

Das Recht am eigenen Bild

Fotografierte Personen haben das Recht, eine Aufnahme zu untersagen!

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

Laut § 201a StGB macht sich strafbar, wer Bild-/Video-/Tonaufnahmen ohne Erlaubnis der/des Betroffenen herstellt u./o. verbreitet!

-- Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe möglich --

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.

Internetsicherheit

Das Internet bietet heute viele einfache und bequeme Möglichkeiten an, Dienstleistungen oder Geschäfte zu tätigen:

- Online-Shopping/E-Commerce
- Bankgeschäfte
- Nachrichten lesen
- Themen recherchieren
- E-Mails verschicken/empfangen
- Kauf von Medikamenten
- Soziale Netzwerke besuchen
- Anmeldung bei Partnerbörsen

Internetsicherheit

Online-Shopping/E-Commerce

- Informieren Sie sich gut über den Anbieter (Identität/Anschrift des Anbieters prüfen)
- Bewertungsprofile oder Internet-Gütesiegel prüfen
- Online-Shop auf Impressum prüfen
- AGB vor dem Kauf durchlesen
- Sichere Zahlungsmethoden verwenden (Kauf auf Rechnung, Bankeinzug, Kreditkarte)
- Sicherheit des verwendeten Gerätes beachten (z.B. beim Smartphone)

Internetsicherheit

Bankgeschäfte

- Sicherheit des verwendeten Gerätes beachten (Smartphone/Laptop)
  - Betriebssystemsoftware auf dem neuesten Stand
  - Firewall und Antivirenprogramm installiert
  - starke Passwörter verwenden (mindestens 12 Zeichen aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen)
  - Zwei-Faktor-Authentisierung verwenden (z.B. Passwort + SMS TAN, Face-ID)
- Banking Apps sollten geprüft sein (IOS-App Store, Google-Play Store)
- Secure-Health-Status prüfen (http**s**…/grüne Anzeige)

<u>Zugangsdaten auf einer gefälschten Website angegeben:</u>

=> Sperren Sie sofort den Zugang zu Ihrem Bankkonto. Nutzen Sie dazu den kostenfreien Sperr-Notruf 116 116. Kontaktieren Sie umgehend ihre Bank. Erstatten sie Anzeige bei der Polizei.

Internetsicherheit

Kauf von Medikamenten

- Deutsche Zulassung bei Wahl der Internet-Versandapotheke
  - Prüfung im Versandapothekenregister auf https://www.bfarm.de/
- Prüfen des Impressums auf vollständige Anschrift der Apotheke
  - Name des Apothekers
  - zuständige Aufsichtsbehörde und Apothekerkammer (gesetzlich vorgeschrieben)
- Sicherheit des verwendeten Gerätes beachten (Smartphone/Laptop)
- sichere Zahlungsmethoden verwenden

Internetsicherheit

Soziale Netzwerke & Partnerbörsen

- Gehen Sie vorsichtig mit ihren privaten Daten um (Fotos, Informationen)
- starke Passwörter verwenden
- Privatsphäre Einstellungen nutzen (Anschrift, Telefonnummer nur bedingt angeben)
- Seien sie skeptisch gegenüber Kontaktanfragen
- alternative E-Mail bei Online-Kontaktbörsen verwenden
- Nicht auf Geldanfragen reagieren (Romance-Scamming)
- Google Rückwärtssuche (Bilder, Namen)

Schutz & Prävention


Quelle: Adobe Stock/Polizei NRW

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 Senioren

- Machen Sie sich mit den Funktionen von PC- und Mobile Devices vertraut sowie deren Internetfähigkeit
- Achten Sie auf entsprechende Vorkommnisse im Internet
- Informieren Sie die Polizei, wenn der Verdacht einer Straftat vorliegt

Video: 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.

POLIZEI
Nordrhein-Westfalen
Dortmund

Vielen Dank für Ihre Aufmerksamkeit

Kriminalprävention Cybercrime
Marcel Wessollek

Tel.: 0231-1327053
E-Mail: marcel.wessollek@polizei.nrw.de