

Grundlagen von Smartphones, Tablets! & Internet-Kriminalität!!!

Das Ziel meiner Präsentation „Der Umgang mit der Digitalisierung“ ist, Menschen zu unterstützen, die wenig Erfahrung mit Smartphones/Tablets haben und diese Geräte nur für grundlegende Aufgaben im Alltag nutzen. Das ist eine sehr sinnvolle und wichtige Aufgabe, gerade für ältere Menschen oder Einsteiger !

Wegen Lizenzen und Urheberrechte, werden nur eigene Bilder oder eigener Text verwendet! Für die Präsentation "Internet Kriminalität" besteht eine Teil-Freigabe Genehmigung durch das Bundesministerium für Sicherheit & BKA!

Inhaltsverzeichnis !

Folie 1-3 Erklärung

Folie 4-13 Allg. Grundwissen und Regeln

Folie 14-27 Einstellungen und Bedienung

Folie 28-40 Internet&Kontoschutz

Folie 41- 61 Internet Kriminalität

Folie 62- Aktuelle Info's (Beantwortung aktueller Fragen von unseren Mitglieder)!

Was tun ab Sechzig!

Digitalisierung ab 60!

Wir leben in einer Zeit, da wissen wir nicht was politisch und wirtschaftlich passieren wird.

Aber was wir mit Sicherheit wissen, die Digitalisierung in allen Bereichen wird sich maßgeblich ändern und wer diesbezüglich stehen bleibt hat verloren!

Ich versuche das etwas einfacher rüberzubringen, ob mir das gelingt weiß ich jetzt noch nicht.

Diesbezüglich gibt es hier und da mal was über eine Online-Schulung im Internet aber eine Zusammenfassung über die Grundkenntnisse für Senioren die ein Handy , Tablet, Telefonie und Heimnetz(WLAN/LAN) für Zuhause sich anschaffen wollen, ist sehr schwer was zu bekommen. Man muss sich alles selbst zusammenstellen und aus eigener Erfahrung handeln. Das einzige ist die Internetkriminalität, da bekommt man was vom BKA!

Allgemein

Gerätetyp und Betriebssystem

Es gibt viele Produkthersteller mit unterschiedlichen Gerätetypen.

Je nach Hersteller bringt ein bestimmtes Betriebssystem das Gerät zum Laufen.

Smartphone > Android

Egal von welchem Hersteller.

Dieses Symbol ist allerdings nicht auf dem Gerät selbst abgebildet. Äußerlich unterscheiden sich solche Geräte nur leicht von den Apple-Geräten.

Verschiedene Hersteller wie Samsung, Huawei, HTC und Google laufen mit Android.

Appel > IOS System!!

Der Hersteller Apple vertreibt nur ein bestimmtes Smartphone bzw. Tablet:
Das iPhone oder iPad.

Diese Geräte laufen mit dem Betriebs-System iOS von Apple.

Bevor ich anfangen, eine wichtige Regel!

Im Umgang mit dem Handy und PC!!!

- 1. Ruhe bewahren**
- 2. Wenn es nicht funktioniert, Hilfe holen(Bekannte, Fachmann**

Fehler können entstehen: (Auch beim Handy)

-Falsche Software durch interne oder externe Einflüsse,
der Mensch selbst durch falsche Eingaben,
Schädliche Software runtergeladen, Händer,
Drittanbieter, Stromausfall, Hardwarefehler.....

Was man selbst machen kann:

- Neustart
- Geräewartung >Einstellungen>Smartphone
- Virens Scanner
- Hersteller, Support, anrufen(Handy Doktor)
- oder strg/alt/entf. Gleichzeitig drücken!(nur beim PC, Tablet, Laptop)

Keine Angst vor dem Handy/PC!

Bestimmtes Grundwissen sollte man haben, über:

Kommunikation-Soziale Medien-Geräten !
(Router/Receiver/TV/ Drucker/ USB/ WLAN/
LAN/Glasfaser/APP's/Magenta/Provider uvm.....

Zuhause >über Internet/WLAN telefonieren!

Außerhalb>nur über Handy-Simkarte

Für unterwegs>Computer/Lapetop/Tablet nur mit
Datenkarte oder 2. Simkarte (gibt es extra Zb. bei Telekom...)

Dabei sollte man die Sicherheit nicht vernachlässigen!!!



Sicherheit

VIERENSCANNER & BEDROHUNGSSCHUTZ

FIREWALL & NETZWERKSCHUTZ

KONTOSCHUTZ

Handy

Auf Einstellungen gehen!

Sicherheit und Datenschutz!

Weitere Sicherheitseinstellungen!

Android Safe Browsing!

„Live-Schutz vor Bedrohungen verwenden“!!!

Die Installation einer Antischadsoftware-App und deren Aktualität kann Dazu beitragen, Ihren PC vor Viren und anderer Schadsoftware zu schützen! (Man kann auch beim Handy einen Externen Virens scanner installieren)!

„Die meisten guten Virens scanner(PC), kann man für 3.5 Geräte kaufen und auch für das Handy benutzen“! >Kosten ca. 65€ bis 100€ im Jahr<

Firewall & Netzwerksicherheit!

Unbefugten Zugriff für Handy und PC!

(Handy wird für Online Banking benutzt oder für Online Bestellungen, Kontenmeldungen & Anmeldung von TV-Privat Sender(Sky, Prime Video, DAZN, Magenta, Netflix....

Firewalls werden häufig verwendet, um sicherzustellen, dass Internetbenutzer ohne Zugriff nicht auf private Netzwerke oder Intranets zugreifen können, die mit dem Internet verbunden sind

Kontoschutz!

(Wichtige Dateien, Dokumente, Online Banking...)

Starkes Passwort, (nicht immer das gleiche, Daten von Familie oder den eigenen Geburtstag, Eigenes Kennzeichen, sollte man nicht nehmen! Fingerabdruck, Gesichtserkennung oder ein sehr starkes Kennwort, sollte man nehmen!!!!)

Checkliste neues Handy!

- **SIM- und Speicherkarte einsetzen**
- **Akku laden**
- **Dein neues Handy einrichten**
- **Daten des alten Handys übertragen**
- **Konten einrichten**
- **Sperrmethode auswählen**
- **Software updaten**

-Welche SIM- und Micro SD-Karte (gibt verschiedene, die zum jeweiligen Smartphone passen, klein oder groß,) kommt auf das Handy an.
(Einschubfach vom Handy, für Mini oder Maxi Simcard)?

-Akku erst laden!

-Dein neues Handy einrichten,

Du hast die SIM- und Speicherkarte eingesetzt und schaltest Dein Smartphone zum ersten Mal ein, der Einrichtungsvorgang kann jetzt beginnen.

Wähle die Sprache aus und verbinde das Telefon mit einem WLAN-Netzwerk, um so Konten verknüpfen und Apps aktualisieren zu können. Hast du keinen Zugang zu einem WLAN-Netzwerk, kannst du diesen Punkt vorerst überspringen.

Halte das Passwort für das WLAN-Netzwerk bereit. Das Standard-Passwort findest du in der Regel auf der Unterseite des Routers.

Abhängig von Modell und Softwareversion können einzelne Schritte der Kurzanleitung variieren.

Daten des alten Handys übertragen

Samsung bietet mit Smart Switch (Datenübertragung)

Um alle Möglichkeiten deines Smartphones nutzen zu können, benötigst du verschiedene Online-Konten, diese kannst du mit deinem Smartphone verknüpfen.“ **Google-Konto** „ zum Beispiel.

Eine aktive Internet-Verbindung ist hierfür vorausgesetzt.

Die Verknüpfung bestehender oder neu angelegter Konten ist auch nach Abschluss der Ersteinrichtung jederzeit möglich.

Passwort für den Sperrbildschirm

Updates zulassen(immer neuester Stand, schützen dein Gerät)

Prepaid: SIM-Karten ohne Vertrag

Volle Kostenkontrolle. Große Flexibilität. Ideal für Preisbewusste. Geeignet auch für Kinder und Jugendliche. Kaufen Sie eine Prepaid-SIM-Karte ohne Vertrag, steht Ihnen ein bestimmtes Guthaben zur Verfügung. Über dieses werden ausgehende Anrufe, SMS und die Nutzung des mobilen Internets abgerechnet. Ist das Guthaben aufgebraucht, laden Sie Ihre Prepaid-Karte wieder auf

**Prepaid-Karten
Verschiedene
Anbieter!**

Systemeinstellungen

Die Einstellungen gehören zur Grundausstattung jedes Smartphones und Tablets.

Sie können nicht gelöscht, sondern lediglich in den Werkszustand zurückversetzt werden.

Die Einstellungen sind in mehrere Bereiche gegliedert, die wieder in mehrere Bereiche aufgeteilt sind.

Dort ist der Zugriff auf zahlreiche Funktionen und Eigenschaften des Geräts möglich.

Typisch sind z.B. diese Bereiche:

- WLAN
- Anzeige
- Speicher

Sie erreichen die Einstellungen über ein Symbol, das wie ein Zahnrad aussieht. Je nach Modell / Version erscheint das Symbol mit leichten Unterschieden.

Dienste und Apps

Einige Dienste sind standardmäßig im Betriebssystem verankert, zum Beispiel:

Anwendungen



- Anrufe / Telefon
- SMS-Nachrichten
- Taschenrechner
- Kalender
- Wetter
- Töne und Mitteilungen
- Geografische Karten (Google Map)

Solche Dienste sind **Anwendungen**, die jeweils einem ganz bestimmten Zweck dienen. Meist können diese ebenfalls nicht gelöscht werden.

Etwas anders verhält es sich mit den **Apps**. Diese können Sie selbst installieren oder entfernen. Doch auch jede App hat einen bestimmten Nutzen. Viele Apps sind je nach Hersteller / Gerät / Modell bereits installiert, darüber hinaus entscheiden Sie selbst welche zusätzlichen Apps Sie benötigen.

Apps suchen und herunterladen

Neue Apps finden Sie im App Store bzw. im Play Store.

Dort sollten Sie darauf achten, ob eine App kostenlos ist oder nicht!

System Zusatz-Info!

Display >>> mit dem Finger von oben nach unten über das Display streichen(1x & 2x)!

Was kommt da zum Vorschein???

Ausschalten>>>

Neustart>>

Notruf

evtl. Medizinische Information!

Besser sehen bzw. erkennen!

Apple

Wählen Sie *Einstellungen* >
Anzeige & Helligkeit.

Bewegen Sie den Schieberegler nach rechts
bzw. links, um die Helligkeit anzupassen.

Bildschirmhelligkeit!

Android

Wählen Sie bei älteren Versionen
Einstellungen > *Ton und Anzeige* >
Anzeige (oder Display & LEDs) >
Helligkeit.

Bei neueren Versionen wählen Sie
Einstellungen > *Anzeige*,
Fingerbewegungen und Tasten >
Helligkeit.

Display einfach mit Finger 2x von oben
nach unten ziehen!

Bewegen Sie den Schieberegler nach
rechts oder links, damit es heller oder
dunkler wird.

Texteinstellungen

Displayeinstellungen können dafür sorgen, die Bildschirmanzeige leichter und besser erkennbar zu machen, z.B. durch größeren Text und höheren Kontrast.

Android

Wählen Sie *Einstellungen und dann je nach Modell / Version Display*.

Oder **Anzeige** oder *Personalisieren oder Eingabehilfen*.

Schließlich kommen Sie zum Eintrag *Schriftgröße und weitere Möglichkeiten wie Displaygröße*.

Apple

Wählen Sie *Einstellungen > Bedienungshilfen > Anzeige & Textgröße*.

Nehmen Sie die für Sie passenden Einstellungen vor.

Gerätewartung!!!

Auf den Smartphones benutzen !!!!!

Kamera!

**Die meisten Geräte haben eine eingebaute Kamera.
Damit können Sie Fotos machen, die Sie später
anschauen und verschicken können.**

Fotografieren, Selfie, Bearbeiten, Weiterleiten!

Foto-Galerie Android>>>

Bildschirmaufnahme oder Screenshot

**Ein Screenshot ist eine Momentaufnahme vom Bildschirm
Ihres Gerätes. Das kann hilfreich sein, um anderen zu zeigen,
was Sie selbst auf Ihrem Gerät zu irgendeinem Zeitpunkt
sehen. Mit der Handkante von links nach rechts über den
Bildschirm streichen bis das Foto einen Ton von sich gibt!
Zu sehen dann in der Datei unter Bilder oder Screenshot(Ordner)**

Android

Erstellen Sie einen **Screenshot**, indem Sie die An/Aus-Taste sowie die Leise-Taste am seitlichen Rand des Geräts gleichzeitig für ca. 2 Sekunden gedrückt halten.

Dann wird kurz eine Vorschau des **Screenshots** eingeblendet.

Oder: Display 2x nach unten & 1x nach links streichen, und schon sieht man rechts das Symbol zum Screenshot, anklicken – fertig!

Screenshot ansehen und nutzen

Eine Bildschirmaufnahme kann genauso verwendet werden wie ein Foto oder jegliches andere Bild. Sie können zum Beispiel den **Screenshot** per E-Mail oder WhatsApp verschicken.

Apple

Sie finden die **Screenshots** unter *Fotos > Medienarten > Bildschirmfotos*.

Android

Sie finden die **Screenshots** unter *Fotos > Alben > Screenshots*. (*Eigene Dateien*)

Lautstärke

Für Ihren Klingelton können Sie die gewünschte Lautstärke bestimmen. Dies betrifft auch andere Töne, mit denen Sie z.B. über eingehende Nachrichten informiert werden.

Android

Wählen Sie ***Einstellungen > Töne oder Ton und Benachrichtigung.***
Bewegen Sie den Schieberegler nach rechts oder links, um die Lautstärke anzupassen.
Oder, Töne und Vibration>>>Lautstärke!
Oder, rechts Lautstärke Taste drücken und dann mit Finger drauf drücken!

Apple

Wählen Sie ***Einstellungen > Töne oder Töne & Haptik.***

Flug-Modus

Im Flugmodus werden die Mobilfunkverbindung, WLAN und Bluetooth abgeschaltet.
Mit Deaktivieren des Flugmodus sind die Verbindungen wieder möglich. Wenn man zum Beispiel in der Nacht Anrufe lieber ausschalten möchte oder um Hintergrundaktivitäten zu verhindern, **die sich auf das Datenvolumen auswirken,** kann man auch den Flugmodus einschalten.

Wählen Sie bei älteren Versionen ***Einstellungen > Verbindungen > Netzwerkverbindungen (oder Drahtlos und Netzwerke).***
Bei neueren Versionen wählen Sie ***Einstellungen.***
Schalten Sie den Flugmodus an bzw. aus. Je nach Modell / Version heißt der Eintrag ggf. „Offline-Modus“.

WLAN und mobile Daten

Ähnlich zur Mobilfunkverbindung eines Handyvertrags stellen Anbieter auch ein Kontingent für mobile Daten zur Verfügung. Damit wird die Nutzung des Internets, also der Online-Dienste möglich.

Mobile Daten (Darauf achten, dass bei der Prepaid Simcard dabei ist)!

Mobile Daten werden für alles beansprucht, was über Anrufe und SMS-Nachrichten hinausgeht. Dies geschieht, wenn Sie über das Internet und Apps Daten empfangen oder senden, zum Beispiel E-Mail, WhatsApp, Browser. (Auch ohne Telefon Sim-Card)!

WLAN

Die mobilen Daten Ihres Geräts bleiben unberührt, wenn sie mit einem WLAN verbunden sind. Dann werden die Daten von einem Router übertragen; zum Beispiel eine Fritzbox oder eine Kabelbox. (Ist Gesichert!!!!)

Der Router unterliegt einem eigenen Vertrag, der ein bestimmtes Daten-Kontingent bereitstellt.

Tipps

Um keine mobilen Daten zu nutzen, muss man eine WLAN-Verbindung nutzen.

Beachten Sie, dass öffentliche WLAN-Netze oft ungesichert sind.

Solche Netze werden zum Beispiel in Bahnhöfen, Kaufhäusern und Restaurants angeboten. Sie benötigen kein Passwort. Wenn Sie diese WLAN-Netze nutzen, sind Ihre Daten nicht geschützt und könnten von Hackern missbraucht werden.

Wenn Sie großen Wert auf Privatsphäre und Sicherheit legen, ist es besser, Ihre mobilen Daten zu nutzen, wenn Sie unterwegs sind.

Zum Beispiel über:

Das Handy oder einer extra Daten Sim-Card der Telekom!

Mobile Daten an- und ausschalten

Sie können die mobilen Daten abschalten, um sicherzugehen, dass darüber kein Verbrauch stattfindet.

Apple

Wählen Sie *Einstellungen* > *Mobiles Netz*.

Schalten Sie die mobilen Daten an oder aus.

Mobile Daten>>>Ein/Aus

Daten-Romaning(Mobile Daten, kann zusätzliche Kosten verursachen!!!!
„Achtung im Ausland“

Android

Wählen Sie bei älteren Versionen *Einstellungen* > *Datennutzung*.

Bei neueren Versionen wählen Sie *Einstellungen*.

Schalten Sie das mobile Netzwerk an oder aus. Je nach Modell / Version heißt der Eintrag „**Mobilfunkdaten**“.

Verbindung>>>
Mobiles Netzwerk>>>Ein/Aus



Soll ich Roaming ein- oder ausschalten?

Wann muss ich Roaming aktivieren?

Wenn Du verreist und Dein Handy im Ausland für Anrufe, SMS oder zum Surfen verwenden möchtest, solltest Du das Roaming aktivieren. Im EU-Ausland fallen dafür keine zusätzlichen Kosten an, in anderen Ländern dagegen solltest Du das Roaming ausschalten, um hohe Kosten zu vermeiden!

Wir raten Dir, das Datenroaming im Nicht-EU-Ausland grundsätzlich ausgeschaltet zu lassen, da Du sonst ungewollt in eine Kostenfalle tappen könntest.

WLAN-Verbindung nutzen

Zwei Schritte sind nötig, um eine WLAN-Verbindung zu nutzen:

- 1) **WLAN einschalten**
- 2) In ein WLAN-Netzwerk einwählen

Eine WLAN-Verbindung findet ohne Kabel statt.
Ihr Gerät ist grundsätzlich mit der entsprechenden Funktion ausgestattet.

Apple & Android

Wählen Sie *Einstellungen* >
WLAN.

Schalten Sie die WLAN-
Verbindung „An oder Aus.“

2) In ein WLAN-Netzwerk einwählen

Zusätzlich zur aktivierten WLAN-Funktion Ihres Geräts muss ein Router vorhanden sein, der das WLAN-Netzwerk bereitstellt.

Die Übertragung zum Internet geschieht dann im Router, mit dem Ihr Gerät verbunden sein muss.

Apple & Android

Wählen Sie *Einstellungen* >
WLAN.

Wählen Sie den entsprechenden
Netzwerknamen aus und geben
Sie das erforderliche Passwort
ein.

Einstellung

„WLAN“

Sicheres Passwort

Jeder Router wird mit einem Passwort ausgeliefert. Bei Ihrem Router zu Hause sollten Sie dieses Passwort erneuern und eine eigene Kombination aus Buchstaben, Zahlen und anderen Zeichen wählen.

Internet?

-**Hypertext-System**, das über das Internet abgerufen werden kann.

World-Wide-Web
(wörtlich: weltweites Netz)

-**HTTPS und HTTP**? Mit HTTP (Hyper Text Transfer Protocol-Protokoll) oder HTTPS (Hyper Text Transfer Protocol Secure-Sicher) können Daten im Internet zwischen dem Client (Webbrowser) und Server übertragen werden. Der Client sendet dazu eine Anfrage (Request) an den Server, der eine Antwort (Response) an den Client zurückgibt.(OK)

-**Man gibt einfach in Google**, wikipedia ein oder die Internet Adresse und Google erkennt das sofort und öffnet die Webseite!
<https://de.wikipedia.org>

Auf der Google Website gibt es auch einen Inkognito Zugang!!!!--re.oben>>:

LAN/WLAN!

- Von außen, über Telefonleitung, Kupfer herkömmlich oder die Zukunft, Glasfaser!

Daten empfangen:

- Internet, Telefon ,Mail, Daten aus der ganzen Welt (ZB. Telekom, 1&1, oder anderer Provider) **Ext./Int.**

Daten weiterleiten:

- An den Kunden (Wir benutzen den Router für den Zugang ins Internet, WLAN, E-Mails, Telefon

Daten auf mehrere Geräte nutzen:

- Mehrere Telefone, Handys, PCs, Laptops, TV, Drucker, Kameras, Türschlösser und Klingel..... (Bei einem Normalen Router ist natürlich nur eine begrenzte Anzahl an Geräten möglich)!

Schaltplan vom Anschluss eines Router, an ein Privates Heimnetzwerk! Ext./Int.

-Heimnetz:

-Int: Mit allen Geräten verbunden

- Ext: Von außerhalb über Google oder Microsoft anmelden und zuhause ins eigene Heimnetzwerk über den Router einloggen!

- Natürlich nur über Passwort oder direktes Codewort, ZB. Bei einer Fernschaltung, oder Kameras direkt über MS/Google(Passwort gespeichert!

Es gibt Router:

- Nur für Glasfaser
- Auch manche alten Router können mit Glasfaser betrieben werden!

Umwandler von optischen Licht zu elektrischem Singnal, für den Router!

Nur Glasfaser Router(Direkt)

Was ist ein ONT bei Glasfaser?

Der Optical Network Termination (ONT) wird auch Netzabschlussgerät genannt und wandelt das optische Licht der Glasfaser in elektrische Signale um, die dann dem Router zugeführt werden. Der ONT wird am Ende der Glasfaserleitung montiert.

Internetzugang in FRITZ!Box einrichten

„Dazu müssen wir in den Router“?

**Einloggen <https://fritzbox> oder Notfall-ID 169.254.1.1 eingeben!
(letzeres geht fast immer)! Anschließend Passwort setzen!!!!**

Assistenten für die automatische Einrichtung wählen!

ID. Nr. steht auch oft auf der Unterseite des Routers!!!

LAN-Anschluss & WEITERE GERÄTE AM ROUTER!

Netzwerkkabel vom Router, an verschiedene Geräte:
PC's-Laptops-TV Geräte-Kameras(bedingt)!

Es können auch sogenannte LAN-Switch Verteiler
Mit mehreren LAN Anschlüsse verwenden!

Weitere Anschlüsse möglich!

WLAN-Repeater(Verstärker)!

TV Receiver/Box(Magenta)!

Antennen/Externe LAN-Server

USB-Geräte, Drucker,

Türschlösser, Smart Home

Kameras uvm.

Repeater!

Zum Beispiel die Fritzbox, es gibt natürlich auch andere Repeater!

WLAN Mesh mit FRITZ!

Mit FRITZ! ist Ihr WLAN auf Knopfdruck immer so groß, wie Sie es brauchen.

Kombinieren Sie Ihre FRITZ!Box mit den intelligenten FRITZ!Repeatern und der Kombi aus FRITZ!Powerline mit WLAN.

So passen Sie das Heimnetz Ihren individuellen Bedürfnissen an und genießen WLAN Mesh mit FRITZ!

Mehr WLAN-Reichweite im Handumdrehen

Der FRITZ!Repeater erhöht besonders einfach und effizient die Reichweite vorhandener Funknetze.

Er ist damit die ideale Lösung für mehr WLAN im ganzen Haus.

Internet-Browser

Der Browser ist eine vorinstallierte App, mit der Internet-Seiten aufgerufen und betrachtet werden können.

Apple heißt der Browser>>Safari!

Android ist Standardmäßig der Chrome(Google) als Browser installiert.

Geben Sie den gewünschten Begriff im Suchfeld ein und wählen Sie aus den Ergebnissen.

Suchmaschine

Mit einer Suchmaschine findet man Inhalte aus dem Internet. Wenn Sie in einem Browser einen Suchbegriff eingeben, verwendet der Browser eine bestimmte Suchmaschine um Ihnen die Ergebnisse anzuzeigen. Mittlerweile hat sich für die Internet-Suche auch der Begriff „**nach etwas googeln**“ eingebürgert.

Es gibt auch andere Suchmaschinen zum runterladen, wie:
Zum Beispiel!

**Bing, Yahoo, AOL, Ask.com,
Ecosia, YANDEX, DuckDuckGo.....**

KONTOSCHUTZ! ZAHLUNGSVERKEHR

**Online-Sicherheit über PC und Handy!
über:**

**TAN/SMS/APP/Kennwort/ Fingerscan
Biometrische Sicherung!**

**BestSign APP oder S-pushTan
oder
Kartenlesegerät für Onlinebanking**

Internetkriminalität

- Überblick
 - Verkauf im Internet
 - Schadsoftware
 - Phishing

Internetkriminalität

- Verkauf im Internet
 - Abo-Fallen
 - Kleinanzeigenbetrug
 - Identitätsdiebstahl

Internetkriminalität

- Abo-Fallen
- Abo-Fallen sind vermeintlich kostenlose oder günstige Angebote, die aber zu hohen Rechnungen oder automatisierten Abbuchungen führen.

Internetkriminalität

- Abo-Falle - Beispiel
 - Lockmittel: Gutschein
 - Dahinter versteckt sich eine Verlosung mit einem „Sonderangebot“ (Abo!)

Internetkriminalität

- Abo-Fallen - Schutzmaßnahmen
- Seien Sie skeptisch bei unglaublich günstigen Angeboten. Quelle: pixabay.com
- Achten Sie auf widersprüchliche oder unklare Beschreibung.
- Geben Sie keine persönlichen Daten (Name, Adresse, etc.) bekannt.
- Kontrollieren Sie die Websites ausführlich (Impressum, AGB, etc.).
- Suchen Sie nach dem Angebot auf www.watchlist-internet.at.
- Handeln Sie nicht unüberlegt.

Internetkriminalität

- Kleinanzeigenbetrug
- Kleinanzeigenportale wie Ebay, Willhaben, Shpock und Co. sind beliebt, um gebrauchte Ware entweder günstig zu kaufen oder verkaufen.
- Kriminelle nutzen gezielt die Anonymität auf diesen Kleinanzeigenportalen.

Internetkriminalität

- Kleinanzeigenbetrug - Varianten
 - **Käuferinnen und Käufer werden Opfer durch**
 - Vorkasse-Trick
 - Treuhandbetrug
 - Liquiditätsbetrug
 - **Verkäuferinnen und Verkäufer werden Opfer durch**
 - Scheckbetrug
 - Trick mit der Track-ID
 - PayPal-Trick

Internetkriminalität

- Kleinanzeigenbetrug - Schutzmaßnahmen
- Seien Sie skeptisch bei überhöhten Zahlungen.
- Wickeln Sie den Kauf bzw. Verkauf persönlich ab und bezahlen Sie direkt bei der Übergabe der Ware und umgekehrt.
- Tauschen Sie keine Ausweiskopien beim Kleinanzeigenverkauf aus.
- Nutzen Sie die Kommunikationsmöglichkeiten der jeweiligen Kleinanzeigen-Plattform.

Internetkriminalität

- Identitätsdiebstahl
- Mit gestohlenen Ausweispapieren (Pass, Führerschein, etc.) können Kriminelle vorgeben eine andere Person zu sein, Konten eröffnen, Einkäufe tätigen und unter falschem Namen Straftaten begehen.

Internetkriminalität

- Identitätsdiebstahl - Beispiele
- Betrügerische
Marktforschungsinstitute
- Betrügerische
Stellenausschreibungen

Internetkriminalität

- Identitätsdiebstahl - Schutzmaßnahmen
- Fügen Sie ein Wasserzeichen ein.
Das Wasserzeichen soll darüber Auskunft geben, dass es sich um eine Kopie handelt, welchem Zweck die Kopie dient, für wen sie bestimmt ist und wann sie erstellt wurde.
- Schwärzen Sie nicht benötigte Informationen.

Internetkriminalität

- Schadsoftware
- Ransomware
 - verschlüsselt Systeme
- Spyware
 - spioniert Systeme aus
- Viren
 - zerstören Systeme

Internetkriminalität

- Schadsoftware - Schutzmaßnahmen

- Installieren Sie Programme nur von offiziellen Websites.
- Öffnen Sie keine Datei-Anhänge deren Herkunft unklar ist.
- Installieren Sie Updates.
- Trennen Sie Administrator- und Benutzerkonten.
- Aktivieren Sie Firewall- und Anti-Viren-Programme.
- Führen Sie regelmäßig Backups durch.

Internetkriminalität

- Phishing
- Phishing ist ein Begriff, der sich aus dem Englischen für „password harvesting“ (Passwort ernten) und „fishing“ (angeln, fischen) zusammensetzt.

Internetkriminalität

- Phishing - Beispiel
- In der Nachrichten wird aufgefordert auf einen **Link** zu klicken.
- Dieser führt zu einer Phishing-Seite, die der Website des nachgeahmten Unternehmens ähnelt.
- Die Opfer sollen sich dort einloggen und/oder ihre Kreditkartendaten eingeben.

Internetkriminalität

- Phishing - Schutzmaßnahmen
- Überprüfen Sie die Absenderadresse.
- Hinterfragen Sie den Inhalt der Nachricht.
- Achten Sie auf Grammatik und Rechtschreibung.
- Kontaktieren Sie das Unternehmen direkt und fragen Sie nach.
- Überprüfen Sie die Internetadresse auf Fehler. (*bawagpks.at* ≠ *bawagpsk.at*)
- Aktivieren Sie in Ihrem Browser den Schutz vor Phishing-Webseiten.

Schutz vor Internetkriminalität

- Schritt für Schritt Anleitungen

- Betrügerische Werbung melden
- Phishing-Schutz einschalten
- Dateien auf Viren überprüfen

Betrügerische Werbung melden

- Facebook – Google – Instagram Seite – Auf 3Pkt. Klicken, sind oft oben rechts!
- Auf die 3 Punkte klicken!
- Auf Werbeanzeige melden klicken!
- Auf Irreführend oder Scan klicken und anschließend auf senden!
- Auf fertig klicken um den Vorgang abzuschließen!

Internet Kriminalität

Internetkriminalität, auch Cyberkriminalität genannt, umfasst alle Straftaten, die unter Ausnutzung von Informations- und Kommunikationstechnik begangen werden. Sie hat in den letzten Jahren stark zugenommen und verursacht hohe Schäden bei Einzelpersonen, Unternehmen und Behörden.

Arten von Internetkriminalität

- **Phishing und Identitätsdiebstahl:** Cyberkriminelle versuchen, durch gefälschte E-Mails, SMS oder Websites an persönliche Daten wie Passwörter, Bank- oder Kreditkartendaten zu gelangen. Die gestohlenen Informationen werden dann für betrügerische Zwecke genutzt.
- **Ransomware-Angriffe:** Die Täter verschlüsseln die Daten eines Computers oder Netzwerks und erpressen die Opfer, indem sie ein Lösegeld für die Freigabe fordern.
- **Malware-Angriffe:** Dies umfasst die Verbreitung bösartiger Software wie Viren, Trojaner oder Spyware, die darauf abzielen, Systeme zu infizieren, Daten zu stehlen oder zu beschädigen.
- **Betrug im Online-Handel:** Kriminelle nutzen betrügerische Online-Shops oder Kleinanzeigenportale, um Vorauszahlungen für nicht existierende Waren zu kassieren.
- **DDoS-Angriffe:** Bei einem Distributed-Denial-of-Service-Angriff werden Computersysteme durch eine massive Überlastung lahmgelegt, wodurch die Dienste nicht mehr erreichbar sind.
- **Cyber-Mobbing und Cyber-Grooming:** Bei Cyber-Mobbing werden Einzelpersonen über digitale Kanäle schikaniert. Cyber-Grooming beschreibt die sexuelle Anbahnung von Kontakten zu Minderjährigen über das Internet.

Beispiele für Internetkriminalität

- **Betrug:**
 - Phishing (gefälschte E-Mails, um Anmeldedaten zu stehlen), Online-Shopping-Betrug und Internetabzocke.
- **Hasskriminalität:**
 - Verbreitung von Hassbotschaften, rassistischen Inhalten, Verleumdung, übler Nachrede und Cyber-Mobbing.
- **Digitale Erpressung:**
 - Verbreitung von Schadsoftware wie Ransomware, die Daten verschlüsselt und ein Lösegeld fordert.
- **Hacking:**
 - Einbruch in Computersysteme, was als "Cracking" bezeichnet wird, wenn es kriminelle Absichten hat.
- **Belästigung:**
 - Cyber-Mobbing, Cyber-Stalking und Cyber-Grooming (Anbahnung sexueller Kontakte mit Kindern im Internet).
- **Verbreitung illegaler Inhalte:**
 - Kinderpornografie und rechtsextreme Propaganda.

Was tun bei einer Straftat?

Strafanzeige erstatten:

Wenden Sie sich an Ihre örtliche Polizeidienststelle. Dort werden die Daten aufgenommen und an spezialisierte Stellen weitergeleitet.

Beweise sichern:

Sichern Sie E-Mails, Chatverläufe und andere digitale Spuren, ohne sie zu verändern, und nehmen Sie diese mit zur Polizei. Screenshots sind ebenfalls eine gute Möglichkeit.

Beratung einholen:

Lassen Sie sich bei Bedarf von einem Rechtsanwalt beraten.

Vorbeugen:

Ein angemessenes Risikobewusstsein und vorbeugende Maßnahmen sind entscheidend.

Wie man sich schützen kann

Vorsicht bei E-Mails und Links: Seien Sie skeptisch gegenüber unbekannten Absendern und klicken Sie nicht unbedacht auf Links.

Software aktuell halten: Installieren Sie regelmäßig Sicherheitsupdates für Ihr Betriebssystem und andere Programme.

- Daten sichern: Erstellen Sie regelmäßig Backups Ihrer wichtigen Daten, die Sie offline speichern.

Starke Passwörter verwenden: Nutzen Sie sichere und einzigartige Passwörter für verschiedene Dienste.

Öffentliche WLANs mit Vorsicht nutzen: Seien Sie vorsichtig, wenn Sie öffentliche WLAN-Netzwerke nutzen

Aktuelle Antworten auf Fragen der Mitglieder!!!
(wird zeitnah beantwortet und aktualisiert)