Online Safety

Young people online

Gemeinsam leben & lernen in Europa e.V.

https://cdn.pixabay.com/photo/2015/12/10/16/39/shield-1086703_960_720.png

Zentrale Fragen:

Was sind die Gefahren?

Wie kann ich sie vermeiden?

Gemeinsam leben & lernen in Europa e.V.

Grundregeln für die Nutzung des Internets:

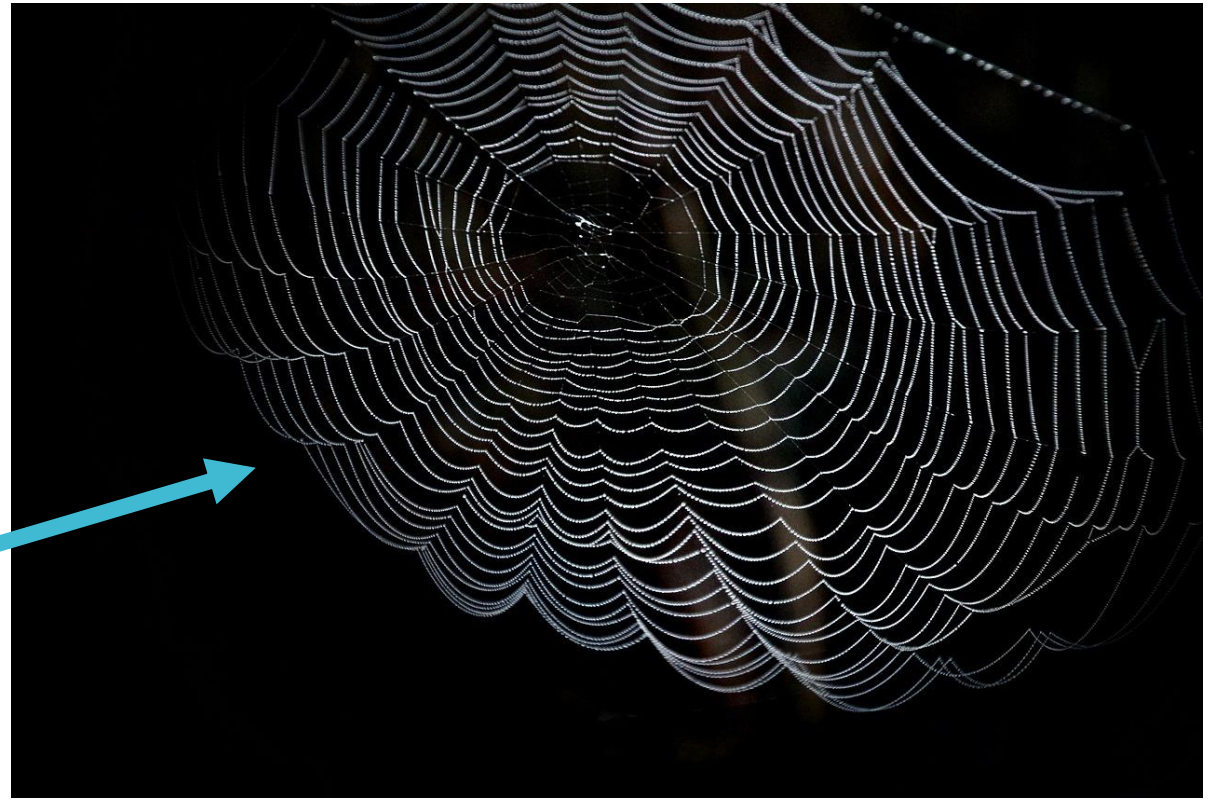
Gemeinsam leben & lernen in Europa e.V.

Definition von „www“:

Woldwide web

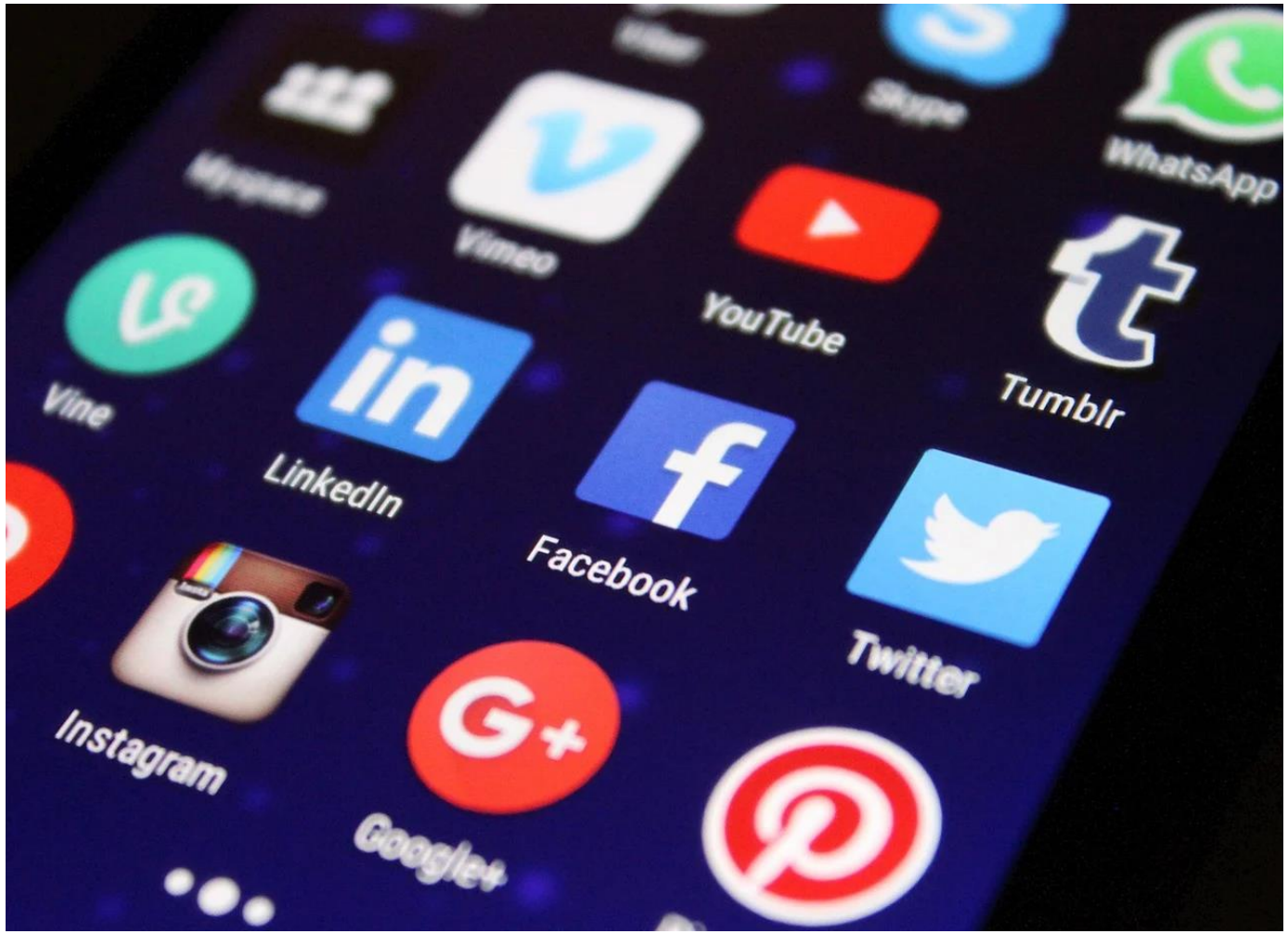
Worldwide bedeutet, dass es **jeder Person** möglich ist zu sehen, was ich im Internet veröffentlicht habe.

Web bedeutet: **alles ist miteinander verbunden**.
Das heißt, wenn ich etwas auf einer Website hochlade, kann es jemand kopieren und woanders erneut hochladen.



https://cdn.pixabay.com/photo/2016/09/27/16/42/cobweb-1698801_1280.jpg

Soziale Medien:



https://cdn.pixabay.com/photo/2015/10/21/08/22/media-998990_1280.jpg

Gemeinsam leben & lernen in Europa e.V.

Einen Account erstellen…

Name?

Geburtstag/Alter?

Wo lebst du?

Deine Telefonnummer?

Etc.

https://cdn.pixabay.com/photo/2015/10/21/08/22/media-998990_1280.jpg

Nur Informationen ausfüllen, die notwendig sind +
Keine **persönlichen Informationen** hinzufügen

<u>Auf keinen Fall</u> solche Benutzernamen wählen:

LenaS.23102005.15

- LenaS → Name
- 23102005 → Geburtstag
- 15 → Alter

Gemeinsam leben & lernen in Europa e.V.

Das www – worldwide web erkunden:

Informationen, die man im Internet preisgibt, können **von jedem weltweit** eingesehen werden.

➡ **Achten Sie darauf, was Sie teilen.**

Nicht vergessen:

Das Internet vergisst niemals.

Selbst wenn Sie ein Foto, bzw. eine Nachricht von Ihnen löschen, werden weiterhin **Kopien von anderen existieren.**

Denken Sie über die Konsequenzen in der Zukunft nach.

- Was wird mein zukünftiger Arbeitgeber über die unvorteilhaften Dinge, die ich geteilt habe, denken?

https://cdn.pixabay.com/photo/2017/04/23/19/30/earth-2254769_1280.jpg

https://cdn.pixabay.com/photo/2017/07/31/21/28/laptop-2561221_1280.jpg

Gemeinsam leben & lernen in Europa e.V.

https://cdn.pixabay.com/photo/2019/04/29/09/33/anonymous-4165613_1280.jpg

Kurze Umfrage:

Wer behauptet von sich, ein starkes Passwort zu haben?
Bitte auf folgende Webseite gehen und
Selbsteinschätzung abgeben:

www.menti.com

https://cdn.pixabay.com/photo/2016/06/03/09/57/password-1433096_960_720.png

Gemeinsam leben & lernen in Europa e.V.

Starke Passwörter nutzen

Man muss sein Passwort nicht regelmäßig ändern.
Es ist besser **starke Passwörter zu nutzen und sie beizubehalten, anstatt einfache Passwörter oft zu wechseln.**

https://cdn.pixabay.com/photo/2019/04/29/09/33/anonymous-4165613_1280.jpg

Ein Passwort sollte folgende Eigenschaften erfüllen:

- **Etwa 12-15 Zeichen besitzen (Eselsbrücken verwenden)**
- **Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen mischen**
- **Für jeden Account ein anderes Passwort verwenden**
- **Keine privaten Informationen miteinbauen**

https://cdn.pixabay.com/photo/2016/02/16/16/57/login-1203603_1280.png

<u>Notiz</u>: Vermeiden Sie es, ein Passwort aufzuschreiben und teilen Sie es <u>nicht</u> mit anderen.

Gemeinsam leben & lernen in Europa e.V.

Brute-force-Methode:

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0-9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a-z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A-Z;a-z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A-Z;a-z;0-9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

https://de.wikipedia.org/wiki/Passwort

https://cdn.pixabay.com/photo/2014/04/03/00/32/padlock-308589_960_720.png

https://cdn.pixabay.com/photo/2016/03/31/18/25/key-1294351_1280.png

Was sind ihre Interessen?

https://cdn.pixabay.com/photo/2019/04/29/09/33/anonymous-4165613_1280.jpg

So viel Information wie möglich über Sie zu bekommen

persönliche Informationen

- Name, Alter…
- politische Haltung
- Wohnort, etc.

kommerzielle Informationen

- Vorlieben/Abneigungen
- Lebenseinstellung
- Bankdaten und Kreditkarteninformationen

https://cdn.pixabay.com/photo/2020/04/04/04/23/bag-5000786__340.png

Diese Daten sind ebenso attraktiv für **Personen, die in der Werbekampagne arbeiten,** da sie **Geld mit den Informationen über Sie machen wollen**.

Gemeinsam leben & lernen in Europa e.V.

Deaktivieren von Programmen, die Daten sammeln

Wenn man eine Website (zum ersten Mal) besucht, wird man gefragt, ob man der **Datensammlung mithilfe von „Cookies"** zustimmt.

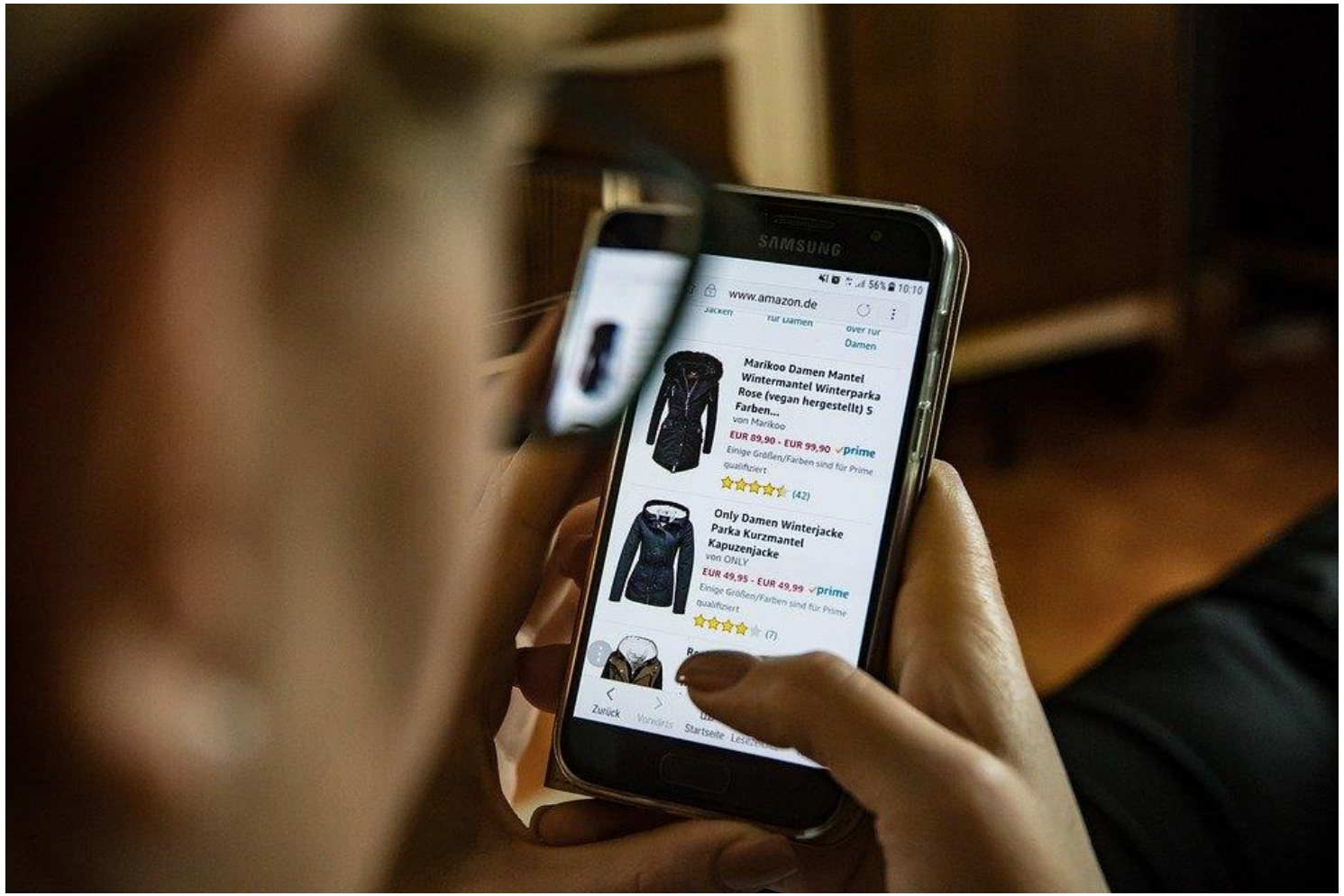
Versuchen Sie nicht alles einfach zu akzeptieren, auch wenn es einen kurzen Moment braucht, um die Einstellungen zu ändern.

➡ **Dies sind die Einstellungen, die Ihre Privatsphäre schützen.**

Werbebetreiber **verstecken** oft besagte Einstellungen auf den Webseiten.
Suchen Sie danach und **aktivieren Sie Ihre Schutzmaßnahmen.**

https://cdn.pixabay.com/photo/2014/04/02/17/06/cookie-307960_1280.png

Online-Einkäufe:



https://cdn.pixabay.com/photo/2017/10/29/17/31/online-2900303_1280.jpg

Gemeinsam leben & lernen in Europa e.V.

Online-Einkäufe:

Viele Menschen benutzen **bargeldlose Bezahlung** aus zwei Gründen:

Es funktioniert **schnell** und **einfach**.

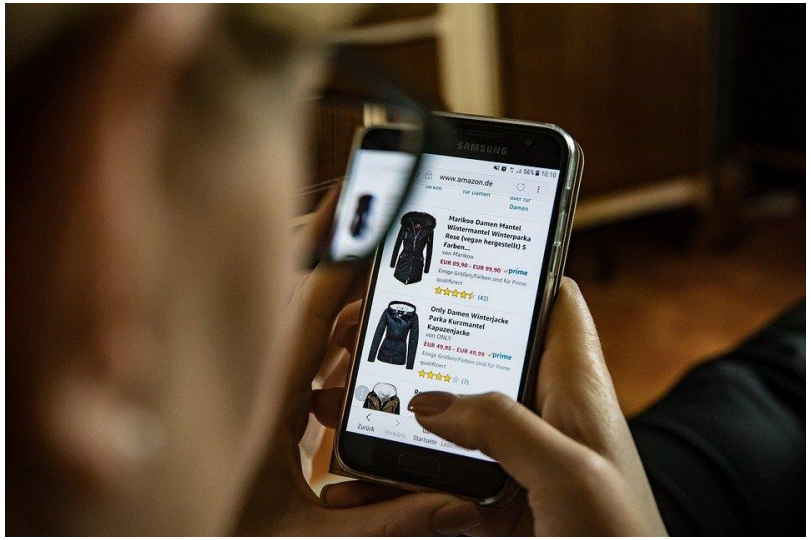
Seit der Covid-19 Pandemie haben bargeldlose Zahlungsmethoden einen weiteren Aufschwung erlebt.

Wannimmer Sie etwas im Internet bestellen, müssen Sie Ihre Kreditkarteninformationen bzw. Ihre Kontodaten angeben. **Hacker lechzen nach dieser Information.**

Geben Sie diese Informationen nur an Webseiten weiter, die **eine sichere, verschlüsselte Verbindung bereitstellen**.

Man kann sie leicht erkennen an:

- einem **s** in "**https:**"
- einem **Schlosssymbol** neben der Adressleiste.



https://cdn.pixabay.com/photo/2017/10/29/17/31/online-2900303_1280.jpg

https://cdn.pixabay.com/photo/2014/04/03/00/32/padlock-308589_960_720.png

Gemeinsam leben & lernen in Europa e.V.

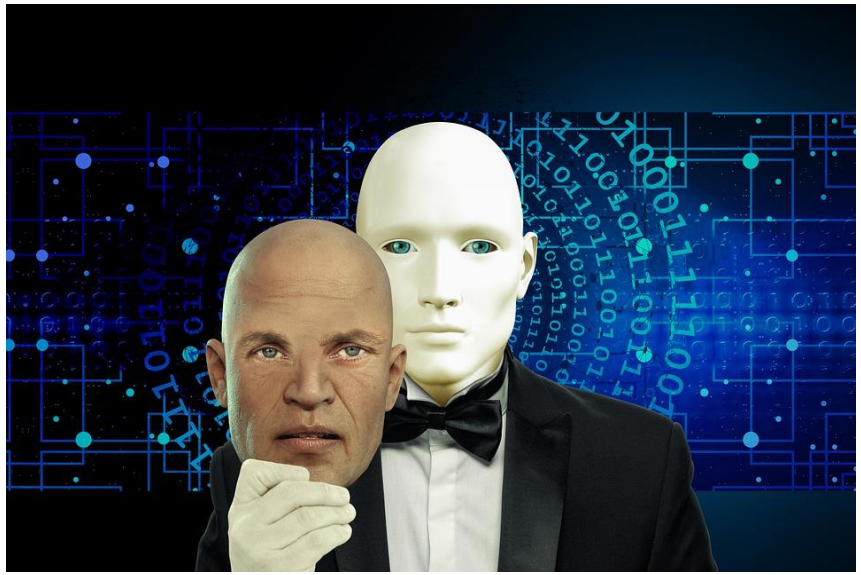
Online-Kontakte:

https://cdn.pixabay.com/photo/2015/11/03/08/58/meeting-1019875_1280.jpg

Gefälscht oder echt?

Wenn man im Internet surft, gibt es viele Accounts mit denen man interagieren kann, **aber nicht alle von ihnen werden von echten Menschen gesteuert**.

Social Bots sind autonome Programme, deren Aufgabe es ist, regelmäßig Beiträge auf bestimmten Websites zu veröffentlichen.
Sie werden hauptsächlich bei Sozialen Netzwerken eingesetzt.



https://cdn.pixabay.com/photo/2020/05/15/12/45/mask-5173443_1280.jpg

Social Bots können außerdem:

- Einen Beitrag liken und kommentieren
- Mit anderen Nutzern interagieren und ihnen antworten
- Untereinander kommunizieren

https://cdn.pixabay.com/photo/2018/05/19/21/36/icons-3414428_960_720.png

Man kann nur schwer zwischen Social Bots und echten Menschen unterscheiden.

Gemeinsam leben & lernen in Europa e.V.

Gefälscht oder echt?

Nicht nur Bots sind verantwortlich für die Verbreitung einer bestimmten Meinung.

Im Internet kann sich jeder ausdrücken, wie er will und dabei seine **Anonymität bewahren**.
Sogenannte **Trolle (Menschen mit bösen Absichten)** nutzen diese Möglichkeit, um bestimmte Meinungen zu verbreiten und **bringen Menschen dazu, ihre Ansichten zu verstärken.**

https://cdn.pixabay.com/photo/2013/07/13/14/05/troll-162078_1280.png

Vorsicht, mit wem Sie interagieren.
Sogar die „echten Menschen" sind nicht immer diejenigen, die sie behaupten zu sein.

➡ **Kommunizieren Sie nur mit vertrauenswürdigen Personen.**

https://cdn.pixabay.com/photo/2018/05/19/21/36/icons-3414428_960_720.png

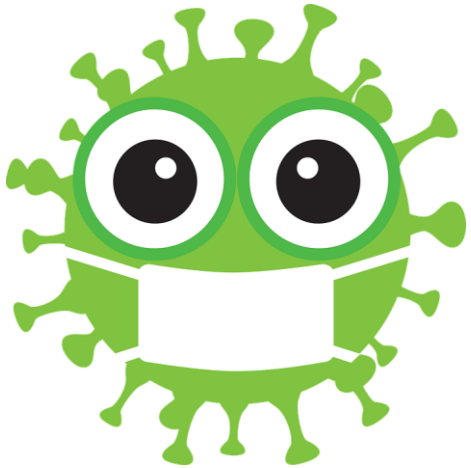
Gemeinsam leben & lernen in Europa e.V.

Was haben diese Grafiken gemeinsam?

Gemeinsam leben & lernen in Europa e.V.

https://cdn.pixabay.com/photo/2013/04/01/21/31/viewpoint-99200_960_720.png

https://cdn.pixabay.com/photo/2020/10/13/20/28/earthworm-5652736__340.png



https://cdn.pixabay.com/photo/2020/04/24/11/44/coronavirus-5086544_960_720.png

https://cdn.pixabay.com/photo/2012/04/13/21/32/rocking-horse-33719_1280.png

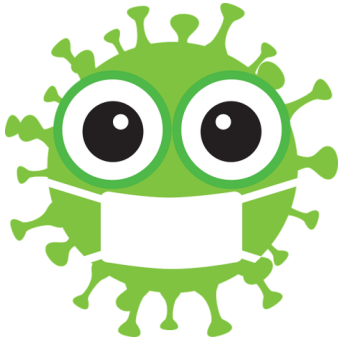
Lösung:

Spyware/Adware

Computerwurm

Malware

= Programme, die das Gerät beschädigen und ausspionieren



Computervirus

Trojanisches Pferd

Downloads

Wenn Sie etwas für Sie interessantes im Internet finden, das Sie downloaden können, tun Sie es vielleicht.

Cyberkriminelle wissen das auch.
Aus diesem Grund verbreiten sie ihre **Malware in Form von gefälschten Dateien oder Apps.**

https://cdn.pixabay.com/photo/2017/02/13/09/53/download-2062197_1280.png

➡ Seien Sie vorsichtig, was Sie auf Ihr Gerät herunterladen.

Laden Sie <u>nichts</u> von einer Webseite herunter, wenn:

- Sie der Seite nicht vertrauen
- Sie wissen, dass der Download illegale Inhalte besitzt

https://cdn.pixabay.com/photo/2017/05/17/19/50/ransomware-2321665_1280.png

**<u>Notiz</u>: Wenn Sie Webseiten mit dubiosen Inhalten besuchen, reduzieren Sie automatisch Ihre Sicherheit.
Damit werden Sie leicht zur Zielscheibe von Hackern.**

Gemeinsam leben & lernen in Europa e.V.

Diese Fragen stellt sich ein Cyberkrimineller:

Hacker

Trojaner

<u>Dreischritt:</u>

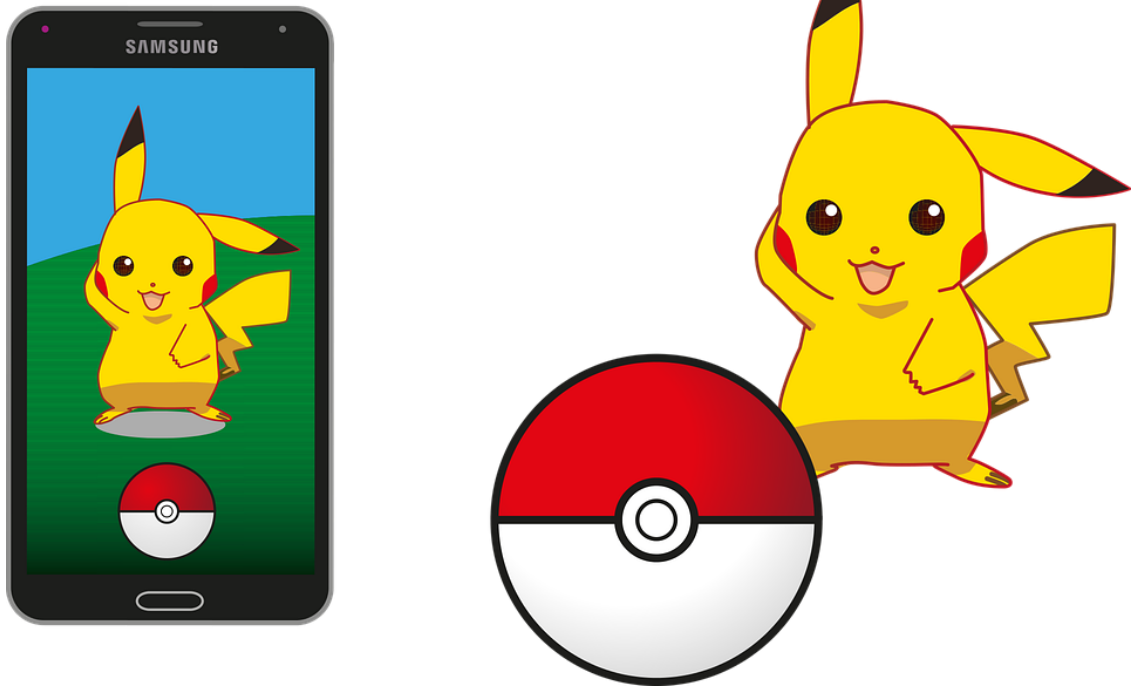
Welches Problem hat meine Zielgruppe?

Welche „Lösung" kann ich ihr bieten?

Wie bringe ich meine Zielgruppe dazu, meine Malware zu akzeptieren?

Gemeinsam leben & lernen in Europa e.V.

Beispiel: Pokémon Go DV-Rechner



- **Bedürfnis** der Zielgruppe:
  Wie stark ist mein Pokémon?
- Cyberkrimineller hat die passende **Lösung**:
  DV-Rechner
- **Das bietet er**:
  Kostenloser Download (schnell und einfach)

Download

DV

https://cdn.pixabay.com/photo/2016/07/29/17/30/pokemon-1555036_1280.png

Gemeinsam leben & lernen in Europa e.V.

QR-Codes

https://cdn.pixabay.com/photo/2013/07/13/10/11/qr-code-156717_1280.png

<u>Das sind die Gefahren:</u>

Man weiß nicht, wohin sie führen

- Unerwünschte Seiten
- Download von Malware

Sie können auf Plakaten leicht überklebt werden

- Kriminelle tauschen den QR-Code aus

Gemeinsam leben & lernen in Europa e.V.

WLAN-Hotspots

WLAN-Hotspots werden von vielen Menschen regelmäßig genutzt.
Man findet sie in Cafés, an Bahnhöfen, in Hotels etc.

Dennoch haben die kostenlosen Hotspots einen **hohen Preis**:
Sie sind sehr attraktiv für Hacker, da sie nicht verschlüsselt sind.

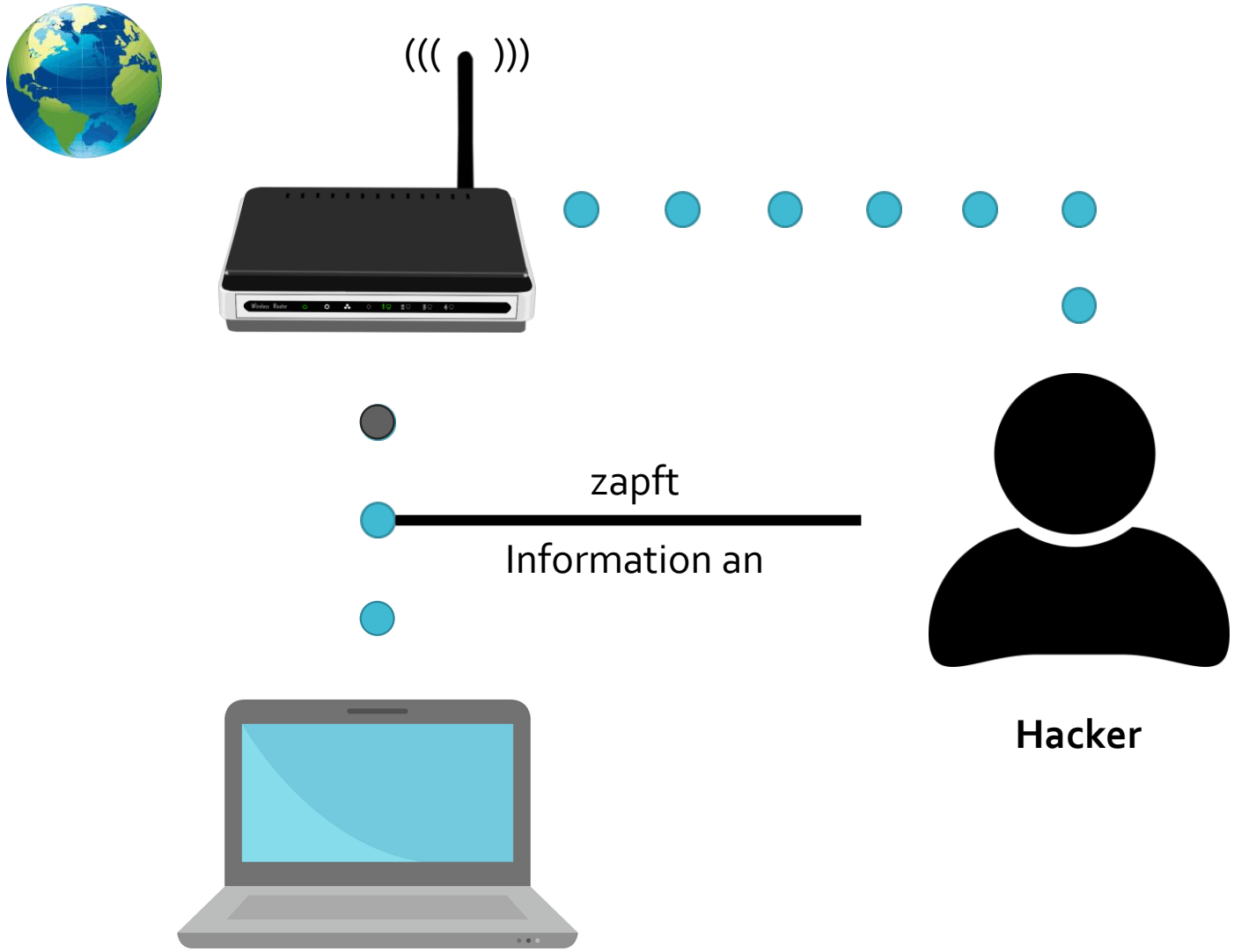
https://cdn.pixabay.com/photo/2013/07/12/15/48/broadband-150348_960_720.png

https://cdn.pixabay.com/photo/2014/12/15/14/02/notebooks-569121_1280.jpg

Alle Daten, die Sie an das Internet übermitteln, können von Cyberkriminellen **angezapft** werden.

Folglich haben diese direkten Zugriff auf **Ihre privaten Dateien, Ihre persönlichen E-Mails oder auch Ihre Bankdaten**.

Gemeinsam leben & lernen in Europa e.V.



Bildquellen:

https://cdn.pixabay.com/photo/2018/11/03/16/44/modern-3792395_1280.png

https://cdn.pixabay.com/photo/2013/04/01/08/38/wireless-98425_1280.png

https://cdn.pixabay.com/photo/2017/02/01/10/00/cartography-2029310_960_720.png

https://cdn.pixabay.com/photo/2016/08/31/11/54/user-1633249_1280.png

Sichere Internetverbindung

Was kann ich tun, um mich zu schützen?

- Nutzen Sie ausschließlich eine sichere Verbindung (**https**).
- Deaktivieren Sie Ihr WLAN, wenn Sie es nicht benötigen

- Deaktivieren Sie die Dateifreigabe Ihres Gerätes; dies können Sie über **Systemeinstellungen bzw. die Systemsteuerung** tun

https://cdn.pixabay.com/photo/2013/07/12/15/48/broadband-150348_960_720.png

https://cdn.pixabay.com/photo/2014/12/15/14/02/notebooks-569121_1280.jpg

➡ **Hacker benutzen Hotspots um:**

- Malware zu verbreiten
- Daten zu stehlen

Gemeinsam leben & lernen in Europa e.V.

Zuguterletzt – schützen Sie sich selbst:

https://cdn.pixabay.com/photo/2015/12/10/16/39/shield-1086703_960_720.png

Antivirusprogramme:

Diese Programme können Sie zwar nicht zu 100 % schützen, aber sie sind in der Lage **Malware** auf eine Minimum **zu reduzieren** und **informieren** Sie, wenn Sie (versehentlich) eine gefährliche Webseite besuchen.
Außerdem **warnen** diese Sie **beim Download einer unsicheren Datei.**

https://cdn.pixabay.com/photo/2017/09/19/16/00/cyber-security-2765707_1280.jpg

Updates:

Halten Sie Ihr Gerät mithilfe von Updates auf dem neuesten Stand.
So wie Programme ihre Sicherheit erhöhen, so verbessern Hacker ihre Systeme, um diese Sicherheit zu durchbrechen.

Gemeinsam leben & lernen in Europa e.V.

https://cdn.pixabay.com/photo/2014/04/02/10/47/computer-304585_1280.png

Fazit:
Auch wenn es einen Moment dauert, Systemeinstellungen zu ändern, Updates durchzuführen und nach sicheren Webseiten/Inhalten/Apps zu suchen…

…nehmen Sie sich Zeit dafür.
Sie schützen damit nicht nur Ihr System, sondern viel wichtiger: sich selbst.

Wer sich ausreichend schützt, kann beruhigt im Internet surfen.

Gemeinsam leben & lernen in Europa e.V.

Quellen:

- https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online
- https://www.dw.com/de/karte-oder-cash-schafft-corona-das-bargeld-ab/av-55699544
- https://praxistipps.chip.de/social-bots-was-ist-das-einfach-erklaert_96529#:~:text=Einfache%20Definition%201%20Social%20Bots%20sind%20automatisierte%20Programme%2C,und%20Kommentieren%20von%20Tweets.%20...%20Weitere%20Artikel...%20
- https://www.englert.one/ein-sicheres-passwort-gestalten
- https://www.heise.de/security/meldung/Passwoerter-BSI-verabschiedet-sich-vom-praeventiven-Passwort-Wechsel-4652481.html
- https://de.wikipedia.org/wiki/Passwort
- https://www.kaspersky.de/resource-center/preemptive-safety/public-wifi-risks

Gemeinsam leben & lernen in Europa e.V.