WORKSHOP - INTERNETSICHERHEIT

Memes

Arbeitsergebnis der 7a

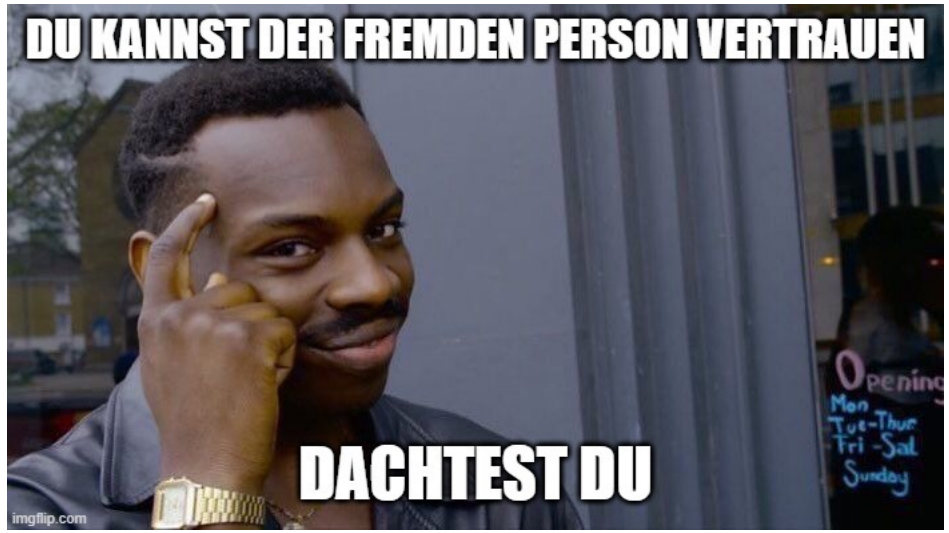
Betreuung: J. Steckhan

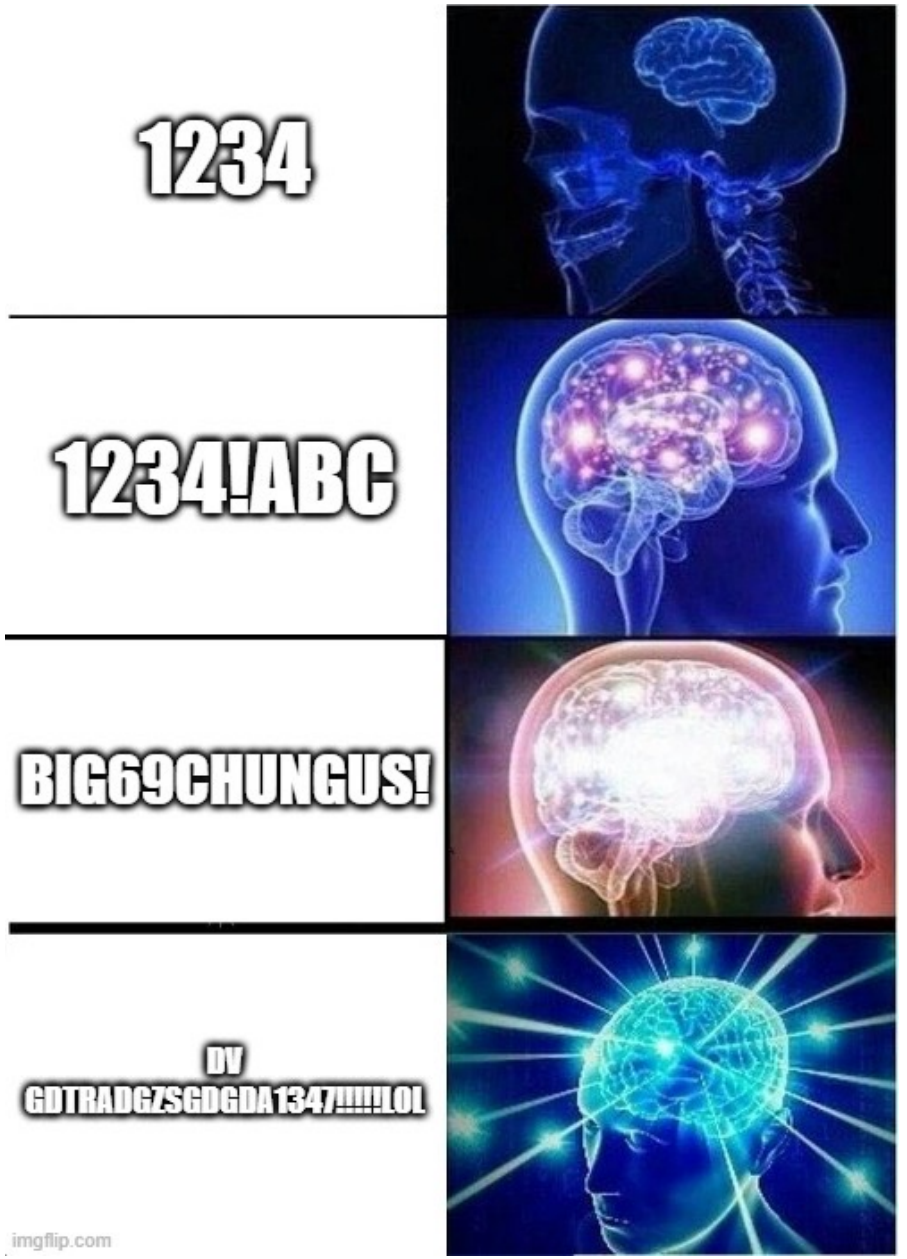
WHEN YOU FORGOT YOUR PASSWORD:


YOU WANT TO VISIT THE WEBSITE
BUT YOU FORGOT THE PASSWORD


DAS IST KEIN VIRUS
DAS SIND DOCH NUR KATZENBILDER
imgflip.com


Dir
Fällt ein
gutes
passwort ein
Du
tipst
es ein
Es
funktioniert
Du hasst
das passwort
nach
3min vergessen

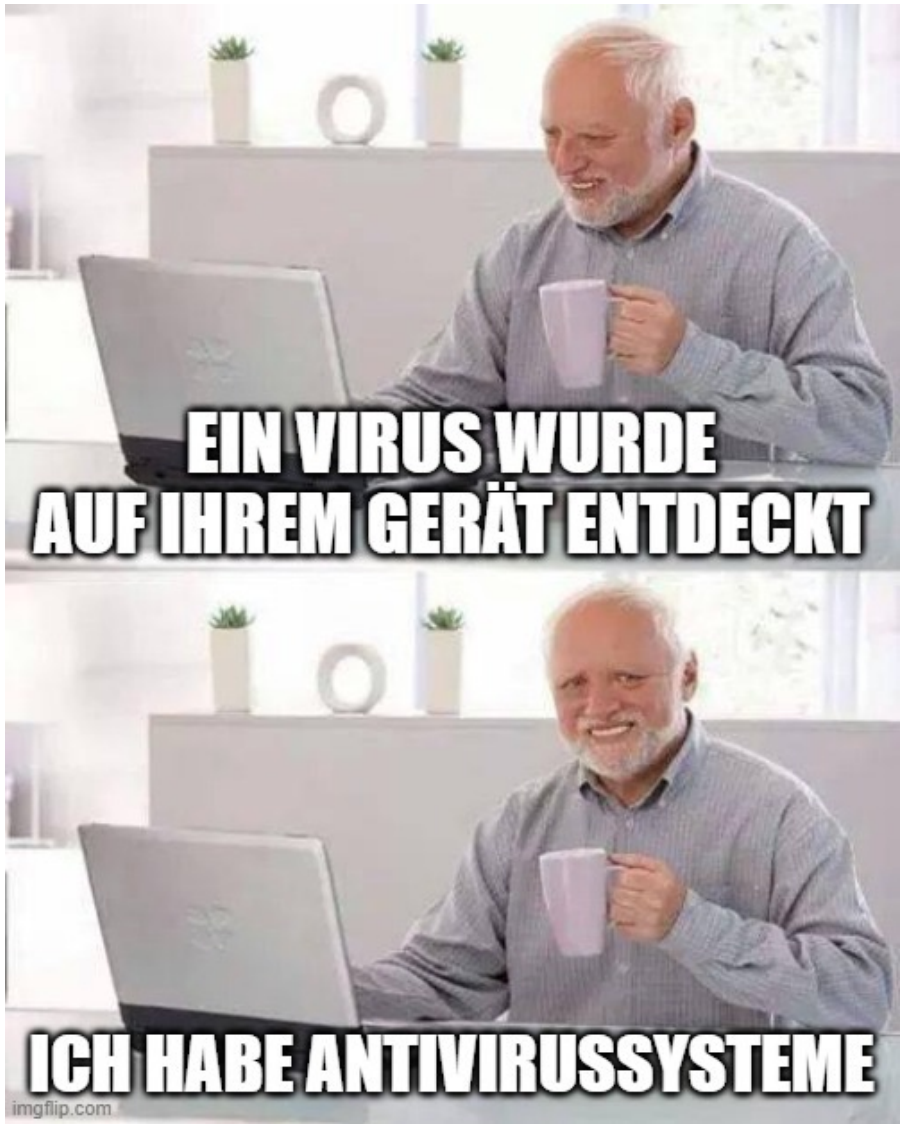

DU KANNST DER FREMDEN PERSON VERTRAUEN
DACHTEST DU
imgflip.com


1234
1234!ABC
BIG69CHUNGUS!
DV
GDTRADGZSGDGDA1347!!!!!LOL
imgflip.com


EY BRO WIE LAUTED
DEIN WLAN PASSWORT?
ER: 9857IOUSDFZNOBS8ZF786S076SF BSD97F6


Gutes
Passwort machen
Lustiges
Passwort machen


ICH


EIN VIRUS WURDE
AUF IHREM GERÄT ENTDECKT
ICH HABE ANTIVIRUSSYSTEME
imgflip.com


Ich bin auf
seriösen Seiten
Ich kriege
ein Virus
WaRuM wUrDe
IcH gEhAcKt?
imgflip.com

Welches Password?

Abc!1234

WORKSHOP - INTERNETSICHERHEIT

Lexikon

Arbeitsergebnis der 7a

Betreuung: J. Steckhan

CYBERMOBBING

- Unter Cybermobbing versteht man, Bedrohung, Belästigungen, Beleidigungen (schriftlich oder auch im Voice Chat), die sich gezielt gegen einzelne Personen richten und wiederholt stattfinden, um die andere Person zu verletzen und zu isolieren. Cybermobbing kann über alle technischen Geräte stattfinden: Smartphones, E-Mails, Websites, Foren, Chats und Communities. Cybermobbing kann für die Betroffenen eine enorme (psychische) Belastung sein!
- Es gibt keine feste Ursache für Cybermobbing. Manchmal gibt es vorher einen Konflikt zwischen einzelnen, manchmal gibt es aber auch gar keine Ursachen und die Betroffenen werden ohne Grund ausgewählt.
- Das kann man tun:

  Erstmal sollte man immer mit jemanden darüber reden und sich Hilfe holen – wenn man sich bei Eltern oder Freunden nicht traut, helfen auch (Online) Hilfsangebote (z.B. Telefonseelsorge, Nummer gegen Kummer, ...)

  Man sollte nicht selbst anfangen sich online aggressiv zu wehren

  Dokumentieren, Leute melden oder blockieren, Gruppen online verlassen

  ggf. auch Anzeige bei der Polizei

CYBERGROOMING

- Cybergrooming ist die gezielte Suche nach und Manipulation von Minderjährigen im Internet. Dies passiert oft auf Social Media Plattformen, in öffentlichen Chatforen, oder Onlinespiele-Plattformen.
- Ziel ist es dabei, das Vertrauen der Kinder zu gewinnen und sie in eine Falle zu locken, um Straftaten (insb. sexuell motivierte Übergriffe) zu begehen.
- Das kann man tun:

  Moderierte Chats und Foren nutzen

  Keine privaten Daten und Informationen in öffentlichen Chats und mit Personen, die man nicht kennt, teilen

  Bei Vorfällen: Personen blockieren, an die Eltern wenden, Hilfe holen, ggf. Fälle dokumentieren und bei der Polizei anzeigen

  Die Seite oder das Programm verlassen

HOAX & FAKE NEWS

- Hoax und Fake News sind Falschmeldungen, die absichtlich im Internet in Umlauf gebracht werden.
- Sie werden verwendet um Aufmerksamkeit zu erzeugen, Angst zu verbreiten, um Meinungen zu beeinflussen oder auch um andere schlecht dastehen zu lassen.
- Das kann man tun:

  Um Fake News zu erkennen, sollte man Informationen aus dem Internet und in den Nachrichten hinterfragen, vor allem seriöse Webseiten lesen (Tagesschau, etc.) und falsche Beiträge melden. Fake News sollte man nicht zusätzlich weiterleiten oder verschicken.

PHISHING

- Phishing bedeutet „Passwort angeln“
- Dabei versuchen die Täter versuchen mit einer E-Mail oder gefälschten Links an eure Daten zu kommen. Sie programmieren z.B. Webseiten, die aussehen wie seriöse Seiten (z.B. Sparkasse Berlin), tatsächlich sind sie aber Fake und die geheimen Daten (Passwörter, etc.), die man dort dann eingibt, werden abgefangen. So kommen die Täter an wichtige Daten und können viel Schaden anrichten.
- Das kann man tun:

  E-Mail, Anhänge und Absender prüfen

  E-Mail löschen, nicht auf die E-Mail antworten und den Versender der E-Mail blockieren

  Keine Links in dubiosen E-Mails öffnen

SICHERE PASSWÖRTER

- Passwörter sind dazu da, um das eigene Konto auf einer bestimmten Plattform, Webseite oder bei einem Spiel zu sichern, Daten geheim zu halten und um nicht gehackt zu werden.
- Ein Passwort sollte eine Kombination aus Buchstaben, Zahlen und Zeichen sein. Man sollte gut drauf achten, dass das Passwort sehr lang oder kompliziert sein soll. Je leichter oder kürzer ein Passwort ist, umso einfacher ist es, in das Konto zu gelangen. Wenn man als Passwort 1234 nimmt, brauchen Hacker sicher nicht mal eine Minute um in das Konto zu kommen.
- Komplizierte Passwörter sind zwar sicher, manchmal kann man sie sich aber schwer merken. Dafür gibt es z.B. Add-Ons oder Passwort-Programme, die Passwörter speichern oder verschlüsseln können. Diese Programme können auch dabei helfen, ein gutes Passwort zu erstellen, wenn man mal keine Idee hat.
- Es wäre nicht schlau, wenn man sein Passwort irgendwo auf seinem Handy oder Laptop speichert. Denn dann muss man nur noch an das Handy kommen und dann hat der Täter direkt alle Passwörter. Es wäre auch nicht gut, wenn du dein Passwort mit vielen Menschen teilst. Man sollte sein Passwort nur für sich behalten.
- Passwörter sollen regelmäßig geändert werden, z.B. jeden Monat, damit es für Hacker schwerer wird.

SOCIAL MEDIA + ÖFFENTLICH GETEILTE INFORMATIONEN

- Zu Social Media gehören digitale Plattformen, mit denen sich Nutzer vernetzen und austauschen können. Mit Social Media kann man neue Leute/Freunde kennenlernen (mit ihnen kommunizieren) und ist immer up to date. Auch Politiker und berühmte Leute haben Social Media, sie benutzen vor allem oft Facebook/Instagram um ihre Fans auf dem Laufenden zu halten.
- Über Social Media werden viele private Informationen geteilt und es ist schwer, einmal verbreitete Dinge wieder aus dem Internet zu löschen. Man sollte daher darauf achten, nicht zu viele Informationen öffentlich zu teilen. Dies kann schnell außer Kontrolle geraten und die Informationen könnten in die falschen Hände geraten. Manche Menschen – auch Erwachsene! – könnten diese Informationen ausnutzen, um andere zu belästigen, anzugreifen, zu stalken, etc.

SPAM

- Spam sind Nachrichten von unbekannten Personen per E-Mail, in Foren oder Chats. Das meiste ist oft Werbung, die man nicht bekommen will. Die Absender versuchen andere Personen zum Kaufen, Lesen, etc. zu motivieren, um so an Geld zu kommen.
- Das kann man tun:

  E-Mails und Absender gut prüfen

  Unbekannte Absender blockieren

  Keine Links in E-Mails von Fremden öffnen

  Virenscanner verwenden

VIREN & TROJANER

- Ein Trojaner ist ein Programm, durch das andere Programme heimlich auf dem Computer installiert werden.
- Computerviren können wie Krankheitsviren einen Computer infizieren. Sie verbreiten sich, wenn infizierte Daten per E-Mail oder über einen Wechseldatenträger wie z.B. einen USB-Stick auf den Computer übertragen werden.
- Durch Viren und Trojaner können andere Personen Kontrolle über den Computer erhalten und Schaden anrichten. Sie können auch Passwörter sammeln oder ändern und so wichtige und vertrauliche Daten zugreifen.
- Das kann man tun:

  Man kann sich vor Viren schützen, in dem man einen Virenschutz installiert, keine dubiosen Internetseiten besucht, keine fremden Links benutzt, E-Mail Anhänge nur von vertrauenswürdigen Quellen öffnet, keine fremden USB-Sticks verwendet und regelmäßige Updates macht.

VIRENSCANNER

- Aufgabe des Virenscanners ist es, Viren aufzuspüren, bevor sie Schaden anrichten. Dabei sucht die Anti-Viren-Software eine Signatur, die jeder Virus besitzt. Der Virenscanner sucht dafür die einzelnen Dateien, eingehende E-Mails und Webseiten nach diesen Signaturen ab.
- Es ist wichtig, regelmäßige Updates zu installieren, damit das Programm die neuesten Viren kennt.