zeit zum

FORSCHEN

EXPERIMENTIEREN WISSEN STAUNEN

CYBERSICHERHEIT

MATHEMATIK IN DER IT

TIPPS FÜR SICHEREN UMGANG

TECHNIKFOLGEN-ABSCHÄTZUNG

EXPERIMENTE ZUM NACHMACHEN

- Caesar-Scheibe
- Gartenzaun-Verschlüsselung
- Passwort-Check
- Steganographie

NACHGEFRAGT

bei Landeshauptfrau Johanna Mikl-Leitner und LH-Stellvertreter Stephan Pernkopf

Welche Rolle spielt die Digitalisierung in Niederösterreich?
Johanna Mikl-Leitner: Die Digitalisierung hat in all unsere Lebensbereiche Einzug gehalten. Wir im Land Niederösterreich haben uns das Ziel gesetzt, das große Potenzial der Digitalisierung für Land und Leute bestmöglich zu nutzen.

Stephan Pernkopf: Digitalisierung eröffnet auch neue Wege, um mit den Bürgerinnen und Bürgern in Kontakt zu treten. Eine gute und rasche Kommunikation war zum Beispiel beim historischen Hochwasser im Jahr 2024 besonders wichtig.

Sind mit der Digitalisierung auch Gefahren verbunden?
Mikl-Leitner: Ja. Die Internetkriminalität hat sich in den letzten Jahren verdoppelt und jeder sechste Cyber-angriff auf Unternehmen in Österreich ist erfolgreich. Wir müssen daher unsere Anstrengungen im Bereich der Cybersicherheit weiter verstärken.

Welchen Beitrag kann hier die Wissenschaft leisten?
Pernkopf: An der USTP St. Pölten gibt es einen starken Schwerpunkt im Bereich Internet Sicherheit. Dort werden jene Kompetenzen aufgebaut, die es braucht, um mit Cyberangriffen umzugehen.
Mikl-Leitner: Eine wichtige Anlaufstelle ist das Haus der Digitalisierung in Tulln. Dort gibt es Angebote zu den wichtigsten Bedrohungsszenarien sowie konkrete Handlungsempfehlungen.

Wie können Kinder und Jugendliche lernen, sicher im Internet unterwegs zu sein?
Mikl-Leitner: Indem sie früh lernen, worauf man achten muss: starke Passwörter, keine persönlichen Daten weitergeben und bei komischen Nachrichten lieber nachfragen. Dieses Thema muss auch verstärkt in unseren Schulen ankommen. Wir müssen Schulen bestmöglich dabei unterstützen, wie ein kompetenter Umgang mit dem Internet gelernt und gelehrt werden kann.

Pernkopf: Im Science Center in Tulln können Kinder ausprobieren, wie das Internet funktioniert, was bei einem Cyberangriff passiert und wie man sich schützt. Wer versteht, wie die digitale Welt funktioniert, ist automatisch sicherer unterwegs – und genau das vermittelt das Science Center auf eine Art, die Kinder und Familien begeistert.

Was wünschen Sie sich, wie die digitale Welt für Kinder in Niederösterreich in Zukunft aussehen soll?
Mikl-Leitner: Ich wünsche mir eine digitale Welt, in der Kinder neugierig sein können, ohne Angst haben zu müssen. Eine Welt, in der sie spielerisch lernen, kreativ sein dürfen und digitale Angebote selbstverständlich und sicher nutzen können.

Pernkopf: Ich wünsche mir, dass digitale Technik Kindern hilft, ihre Talente zu entdecken – egal ob in Naturwissenschaft, Musik, Sport oder Medien. Digitalisierung und auch Künstliche Intelligenz sollen dabei eine Unterstützung sein und keine Hürde – Werkzeuge, die Türen öffnen: zum Ausprobieren, zum Lernen und zum Verstehen, wie die Welt funktioniert.

CYBERSICHERHEIT UND DU

Computer sind überall um uns herum – in Autos, Spielzeugen, Waschmaschinen, Ampeln und natürlich in Handys und Laptops. Oft merken wir gar nicht, dass sie im Hintergrund mitarbeiten. Damit all diese Geräte funktionieren und das tun, was WIR wollen, müssen sie gut geschützt sein. Genau darum geht es bei Cybersicherheit.

Cybersicherheit bedeutet, dass wir Computer, Daten und Netzwerke davor schützen, dass jemand etwas Unerlaubtes damit macht. Stell dir vor, jedes technische Gerät hat eine unsichtbare Tür. Cybersicherheit sorgt dafür, dass diese Tür verschlossen bleibt und nur die richtigen Menschen einen Schlüssel haben.

MIR DOCH EGAL!

Vielleicht hast du schon mal gedacht, dass dich Cybersicherheit nicht betrifft. Aber: Nutzt du ein Handy oder einen Computer? Hast du einen E-Mail-Account? Schreibst du Nachrichten an deine Freunde? Habt ihr einen Staubsaugerroboter? Hast du schon einmal etwas im Internet gekauft? Nutzt du Apps am Handy?

Dann betrifft dich Cybersicherheit und wahrscheinlich machst du auch schon vieles, das genau in diesen Bereich fällt.

Das alles ist Cybersicherheit:
- du verwendest Passwörter
- du installierst Updates
- du klickst NICHT auf komische Links in Nachrichten
- euer WLAN hat ein Passwort
- du installierst ein Virenschutzprogramm
- du erlaubst Apps nicht alles
- ...

Ohne Cybersicherheit wäre das Internet ein Ort, an dem vieles nicht funktionieren würde und unfair wäre.
Cybersicherheit ist also kein kompliziertes Technikthema, das nur Erwachsene betrifft. Es ist ein Teil deines Alltags, genauso wie du die echte Tür eurer Wohnung ja auch zusperrst.

WORAUS BESTEHT EIN COMPUTER?

Ein Computer besteht aus zwei Teilen: Hardware und Software.

Die **Hardware** ist alles, was wir sehen und angreifen können: Bildschirm, Maus, Tastatur, Kamera oder der Akku. Und auch der Computer oder Laptop selbst.

Die **Software** sind Programme und Apps, die im Computer oder Handy „drinnen wohnen". Sie sagen dem Computer, was er tun soll, etwa wie ein Spiel funktioniert, wie man einen Weg findet oder wie man eine Nachricht schreibt. Ohne Software wäre ein Computer wie eine Hülle ohne Inhalt.

Für Cybersicherheit spielt dieser Unterschied eine große Rolle, weil beide auf unterschiedliche Weise geschützt werden müssen. Die Hardware muss z.B. vor Diebstahl, Zerstörung oder Veränderung geschützt werden. Wenn jemand einen USB-Stick in einen fremden Computer steckt, kann er Schadsoftware einschleusen, die den Computer kaputt macht.

Cybersicherheit sorgt dafür, dass niemand etwas Verbotenes mit Computern oder Handys macht. Sie funktioniert wie ein unsichtbares Schloss, das nur die richtigen Menschen aufsperren können.
Du nutzt Cybersicherheit jeden Tag, zum Beispiel mit Passwörtern oder wenn du nicht auf komische Links klickst. Ohne Cybersicherheit wäre das Internet ein gefährlicher und unfairer Ort.

FUN FACTS

Der erste bekannte **Computer „Bug"** wurde 1947 entdeckt. Es war tatsächlich eine Motte, die in einem Computer steckte und einen Schaltkreis blockierte! Seitdem nennt man Fehler in Computern oder Programmen Bugs, auch wenn heute keine echten Insekten mehr Schuld sind.

Die erste Computermaus bestand aus Holz.

„**123456**" ist eines der häufigsten Passwörter der Welt. Aber leider auch eines der unsichersten.

Bei der Software ist es wichtig, dass die Programme fehlerfrei und aktuell sind, damit Angreifende keine Schwachstellen ausnutzen können. Wenn z.B. ein Programm nicht aktualisiert wird, können Angreifer eine bekannte Schwachstelle nutzen, um Daten zu stehlen.

WAS MACHT CYBERSICHERHEIT?

In der Cybersicherheit gibt es drei wichtige Ziele, die zusammen dafür sorgen, dass Computer und Daten zuverlässig geschützt sind:

Verfügbarkeit

Computer und Daten sollen dann verfügbar (da) sein, wenn man sie braucht. Stell dir vor, du willst ein Online-Spiel starten, aber der Server ist kaputt oder jemand blockiert ihn absichtlich. Dann ist das Spiel nicht verfügbar. Cybersicherheit sorgt dafür, dass Systeme nicht ausfallen, dass sie repariert werden können und dass niemand sie absichtlich lahmlegt. Auch Backups fallen in diesen Bereich. Das bedeutet, dass du deine Informationen (Daten) an mehreren Orten speicherst. So sind sie auch dann noch da, wenn ein Gerät kaputtgeht. Backups sind wie ein Sicherheitsnetz und deshalb ein zentraler Teil der Verfügbarkeit in der Cybersicherheit.

Vertraulichkeit

Viele Informationen sind privat und sollen nur von den Personen gesehen werden, die sie sehen sollen.

So wie du dein Tagebuch nicht jedem zeigst, sollen auch deine Daten, Fotos, Nachrichten, Passwörter, privat bleiben. Cybersicherheit schützt diese Informationen davor, dass Fremde sie lesen oder stehlen. Beim Beispiel vom Online-Spiel würdest du ein geheimes Passwort für deinen Account verwenden, sodass niemand deinen Punktestand löschen kann.

Integrität

Integrität bedeutet, dass Daten echt und unverändert bleiben. Stell dir vor, jemand würde heimlich deine Hausaufgaben ändern, das wäre unfair. Oder wenn du jemandem eine Nachricht schickst, soll sie genauso ankommen, wie du sie geschrieben hast und nicht verändert oder verfälscht. Cybersicherheit stellt sicher, dass niemand heimlich etwas an Daten oder Programmen manipuliert.

Cybersicherheit hilft also, unsere Geheimnisse zu schützen und dafür zu sorgen, dass wir Computern vertrauen können.

FORSCHUNG FÜR SICHERE COMPUTER

An der USTP in St. Pölten wird erforscht, wie digitale Systeme wirksam vor Cyberangriffen geschützt werden können. Dazu zählen sichere Lernplattformen, Programme zur automatischen Erkennung von Hasskommentaren sowie Schutzmaßnahmen für vernetzte Systeme wie Stromnetze und Lieferketten. Dafür entwickeln Forschende unter anderem Computerprogramme, die automatisch ungewöhnliches Verhalten in Netzwerken erkennen, sowie Lernmaterialien, mit denen Lehrkräfte Cybersicherheit verständlich vermitteln können.

Die Forschenden schauen sich aber nicht nur die Technik an, sondern auch wie Menschen sich verhalten, denn viele Sicherheitslücken entstehen nicht durch kaputte Computer, sondern durch das, was Menschen tun oder übersehen.

Die **USTP University of Applied Sciences St. Pölten** beschäftigt sich mit aktuellen Fragen der Cybersicherheit und der Künstlichen Intelligenz.

FH-Prof. Dr. techn. Dipl.-Ing. Peter Kieseberg hat Technische Mathematik an der TU Wien, **FH-Prof. Mag. Dr. Simon Tjoa** Wirtschaftsinformatik an der Universität Wien studiert. Gemeinsam arbeiten sie am Institut für IT Sicherheitsforschung. Ziel ihrer Forschung ist es, Angriffe frühzeitig zu erkennen, sensible Daten zu schützen und technische Systeme widerstandsfähiger zu machen.

CAESAR SCHEIBE

EINFACHE HISTORISCHE VERSCHLÜSSELUNG

DAS BRAUCHST DU:

- Vorlage der zwei Caesar-Scheiben
- Schere
- ev. Karton
- Musterbeutelklammer

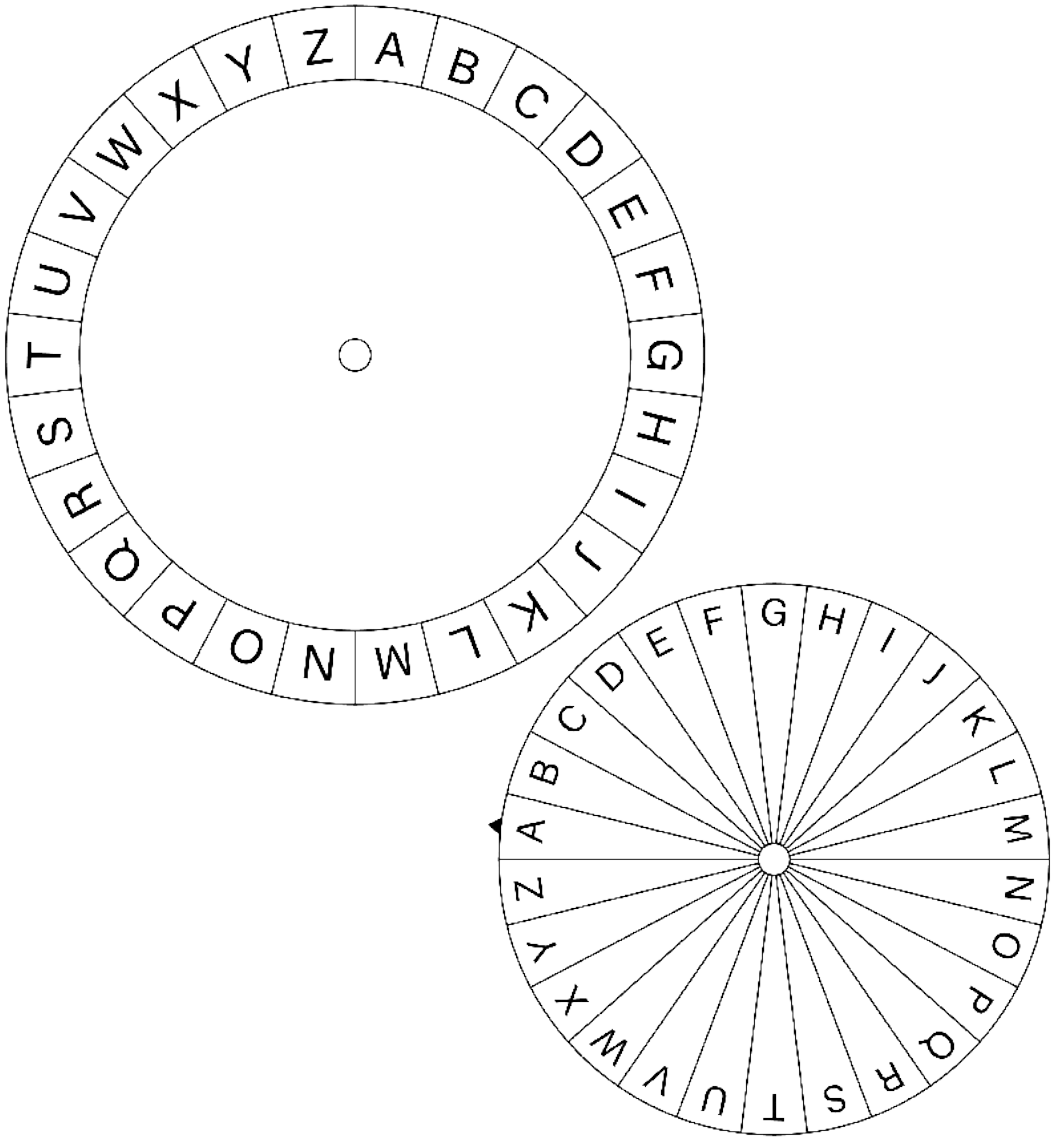
01 Schneide die Caesar-Scheiben aus. Du kannst sie auf einen Karton kleben, damit sie stabiler sind.

02 Stich jeweils ein Loch in die Mitte der Scheiben und stecke die Musterbeutelklammer durch.
Deine Caesar-Scheibe ist fertig.

03 **Verschlüsseln:**
Wähle den Schlüssel. Er gibt an, um wieviele Stellen die innere Scheibe verschoben werden muss.
z.B. +3 bedeutet, die Scheibe wird um 3 Stellen im Uhrzeigersinn verschoben.
A → D, B → E, C → F
Schreibe dein Geheimwort auf und verschlüssele es.

z.B. NORI → QRUL

04 **Entschlüsseln:**
Gib das verschlüsselte Wort und den Schlüssel (z.B. QRUL +3) weiter. Die/der Empfänger*in* schiebt jetzt die innere Scheibe um 3 Stellen im Uhrzeigersinn weiter. Sucht auf der äußeren Scheibe die Buchstaben und notiert, welche Buchstaben sie auf der inneren Scheibe ergeben. So entschlüselt ihr das Geheimwort.



WIESO?

Die Caesar-Verschlüsselung ist ein sehr einfaches Verschlüsselungsverfahren, bei dem jeder Buchstabe im Alphabet um eine feste Anzahl von Stellen verschoben wird. Julius Caesar nutzte diese Methode schon im alten Rom, um geheime Nachrichten zu schützen. Obwohl sie heute leicht zu knacken ist (es gibt nur 25 mögliche Verschiebungen) eignet sie sich gut, um die Grundlagen der Kryptografie zu erklären.

WAS IST DAS EIGENTLICH?

HASH

Mit einer Hashfunktion kann man prüfen, ob eine Datei unverändert geblieben ist. Sie erzeugt aus einer Datei einen kurzen, eindeutigen Fingerabdruck. Schon eine winzige Änderung am Dateiinhalt führt zu einem komplett anderen Hashwert.

RAINBOW TABLE

Eine Rainbow Table ist eine vorberechnete Tabelle von Hashwerten, die verwendet wird, um Passwörter schneller zu knacken. Sie spart Rechenzeit, indem viele mögliche Passwörter und deren Hashes bereits im Voraus berechnet wurden.

BRUTE-FORCE-ANGRIFF

Bei einem Brute-Force-Angriff werden systematisch alle möglichen Passwort oder Schlüsselkombinationen ausprobiert, bis die richtige gefunden ist. Diese Methode ist einfach, aber zeitaufwändig und wird durch starke, lange Passwörter deutlich erschwert.

REVERSE-ENGINEERING bezeichnet die Analyse von Software oder Hardware, um deren Funktionsweise ohne Zugriff auf die Originaldokumentation zu verstehen. Man will herausfinden, wie etwas funktioniert oder aufgebaut ist. In der Cybersicherheit wird das zur Schwachstellenanalyse und auch von Angreifenden zum Finden von Sicherheitslücken eingesetzt.

ZERO-DAY-EXPLOIT nutzt eine Sicherheitslücke aus, die dem Hersteller noch nicht bekannt ist und für die es daher noch keinen Patch (Fehlerbehebung) gibt.

PASSWORT-TRICKS 1

TIPPS FÜR EIN GUTES PASSWORT

Je komplizierter es ist, dein Passwort zu knacken, desto sicherer sind deine Daten. Deshalb sollte ein Passwort immer so lang wie möglich sein.
Es gibt verschiedene Tricks, die helfen, ein gutes Passwort zu erstellen.
Und es sich auch zu merken:

01 Ersetzen-Trick
Dazu werden Buchstaben durch Sonderzeichen und Zahlen ersetzt. So kann zum Beispiel aus einem „E" ein „3" werden, oder aus einem „S" wird das Sonderzeichen „§".
Beispiel: Passwortsicherheit = Pa§sw0rts/ch3rhe1t

02 Satz-Trick
Denke dir einen Satz aus, den du dir leicht merken kannst. Nun nimmst du von den einzelnen Wörtern immer den Anfangsbuchstaben sowie die Zahlen und Sonderzeichen und fügst diese zu einem neuen Wort zusammen.
Beispiel: Heute Nachmittag lese ich das 6. ForscheN-Magazin! = Hnlid6.F-M!

03 Wort-Trick
Eine weitere Möglichkeit dir ein sicheres Passwort zu erstellen, ist das Aneinanderreihen von Wörtern. Nimmst du dir drei Worte, die in keinem logischen Zusammenhang stehen, ergibt das ein sehr langes und sicheres Passwort.
Beispiel: FußballPasswortsicherheitBaum

04 Passwörter variieren
Setze nie überall das gleiche Passwort ein.
Wenn eines geknackt ist, sind alle anderen Dienste auch nicht mehr sicher.

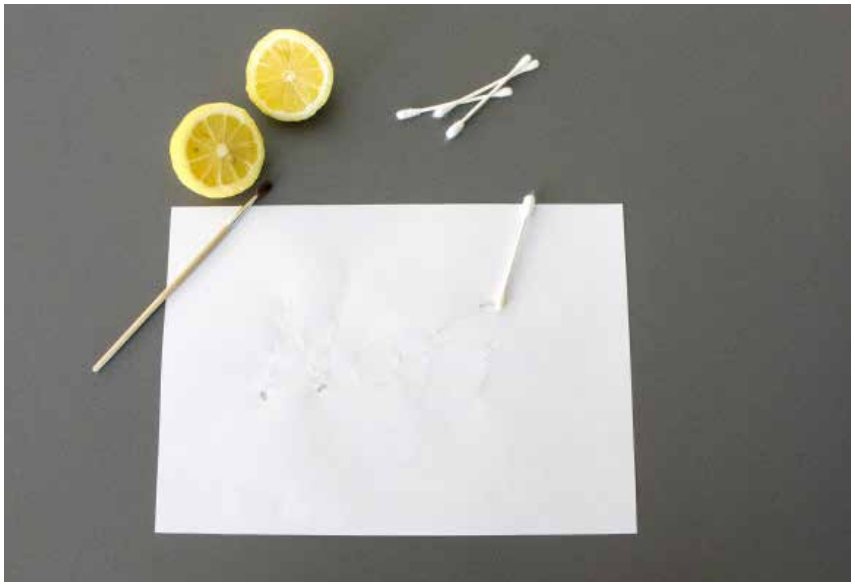
Quelle: https://mecodia-medienkompetenz.de/materialien/anleitung-wie-erstelle-ich-ein-sicheres-passwort-das-ich-mir-merken-kann/

UNSICHTBARE TINTE

ANALOGE STEGANOGRAPHIE

DAS BRAUCHST DU:

- Zitrone, Zitronensaft
- Wattestäbchen oder Pinsel
- Blatt Papier
- Backrohr oder Bügeleisen



01 Schneide die Zitrone in zwei Hälften oder presse den Zitronensaft in ein Glas. Du kannst auch gekauften Zitronensaft verwenden.

02 Tupfe mit einem Wattestäbchen oder einem Pinsel in den Zitronensaft und schreibe damit deine geheime Botschaft auf das Blatt Papier. Lasse das Papier trocknen.

03 Um die Botschaft wieder sichtbar zu machen, musst du das Blatt heiß machen.
Dazu kannst du es:
- heiß bügeln. Vorsicht, lass das Bügeleisen NIE auf dem Papier oder Tisch stehen!
- in den vorgeheizten Backofen legen (ungefähr 200 Grad). Nach 10-20 Minuten wird die Tinte sichtbar.

ACHTUNG HEISS!

WIESO?

Die unsichtbare Tinte funktioniert, weil Zitronensaft viele Kohlenhydrate enthält, die hohe Temperaturen nicht vertragen. Sie beginnen zu verkohlen, ähnlich wie Holz wenn es verbrennt. Deshalb bleibt die Schrift zuerst unsichtbar und färbt sich erst beim Erhitzen.

In der digitalen Welt gibt es Steganographie:
Steganographie bedeutet, dass man eine Nachricht so versteckt, dass niemand merkt, dass überhaupt eine Nachricht da ist. Gerade in großen Bildern kann man sehr leicht viele Daten verstecken, ohne dass jemand merkt, dass überhaupt eine Geheimbotschaft übertragen wird.
Die Nachricht ist versteckt und nicht verschlüsselt. Nur Eingeweihte wissen, dass überhaupt etwas geschrieben wurde.

MATHEMATIK IN DER IT

Wieso manche Zahlen braver sind als andere und warum eine Rechnung manchmal so schwierig wie möglich sein soll.

Mit Zahlen, Mustern und Rechenregeln können Informationen so versteckt werden, dass nur die richtigen Menschen sie lesen können. Ohne Mathematik gäbe es keine sicheren Schlösser für Computer, Handys oder das Internet.

KOMBINATORIK

Kombinatorik beschäftigt sich damit, wie viele mögliche Kombinationen von Dingen es gibt. Genau das ist entscheidend für die Sicherheit von Passwörtern.

Wenn ein Passwort aus 10 Zeichen besteht und jedes Zeichen 62 Möglichkeiten hat (A–Z, a–z, 0–9), dann gibt es **839.299.365.868.340.224** mögliche Passwörter (mehr als 839 Billiarden!) – eine gigantische Zahl an Möglichkeiten.

Je mehr Stellen ein Passwort hat und je mehr Zeichen man benutzen darf (Buchstaben, Zahlen, Sonderzeichen), desto mehr Kombinationen entstehen.

Für Hacker wird es dadurch viel schwieriger, das richtige Passwort zu erraten, weil sie unglaublich viele Möglichkeiten ausprobieren müssten. Darum müssen Passwörter lang und aus vielen verschiedenen möglichen Zeichen bestehen.

PRIMZAHLEN

Stell dir vor, du sicherst eine geheime Nachricht mit einer Rechnung, die gelöst werden muss, um sie zu lesen. Dann möchtest du, dass diese Rechnung so schwierig wie möglich ist, richtig?

Es gibt Rechnungen, die die stärksten Computer und Mathe-Genies nicht lösen können. Doch dafür brauchst du besondere Zahlen. Welche, die nicht so brav wie normale Zahlen sind.

Primzahlen sind solche besonderen Zahlen. Sie lassen sich nur durch 1 und sich selbst ohne Rest teilen. Beispiele sind 2, 3, 5, 7, 11. Die Zahl 4 ist zum Beispiel keine Primzahl, weil man sie auch durch 2 teilen kann.

Zwei große Primzahlen kann man leicht miteinander multiplizieren – aber vom Ergebnis wieder die ursprünglichen Primzahlen herauszufinden, ist extrem aufwändig.

Es ist wie wenn du zwei Farben mischst: blau und gelb ergibt grün. Das Mischen ist einfach. Aber aus dem fertigen grün herauszufinden, welche zwei ganz genauen Blautöne und Gelbtöne du verwendet hast, ist fast unmöglich. Genau diese Einweg-Eigenschaft macht Verschlüsselung sicher.

Und so wird das in der Cybersicherheit angewendet: Wenn du eine Website besuchst, wählt der Server zwei sehr große Primzahlen. Er multipliziert sie zu einer riesigen Zahl. Diese Zahl darf jeder sehen, aber niemand kann sie in die Primzahlen zurückrechnen. Nur wer die beiden Primzahlen kennt, kann die Nachrichten entschlüsseln.

Deine Daten bleiben sicher, weil niemand die Primzahlen erraten oder zurückrechnen kann.

Ja, Mathematik ist manchmal echt anstrengend.
Aber sie ist für viele spannende Anwendungen im Internet notwendig und die Grundlage für unser digitales Leben.

Wer Mathe kann, hat Superkräfte, die im echten Leben richtig was bringen!

TIPPS

für einen sicheren Umgang mit Internet, Smartphone & Co.

Persönliches geheim halten.
Wohnadresse, Handynummer, E-Mail-Adresse etc. gehen Fremde im Internet nichts an! Halte deine Passwörter auch vor Freund*innen* geheim.
Checke regelmäßig die Privatsphäre-Einstellungen in deinen Sozialen Netzwerken, sie ändern sich immer wieder.

Das Internet vergisst nicht!
Veröffentliche keine Fotos, Videos oder Texte, die dir oder anderen unangenehm sein könnten. Wurden Inhalte einmal im Internet verbreitet, ist es fast unmöglich, sie wieder zu entfernen!
Das Veröffentlichen oder Verschicken von Fotos oder Videos, die andere Personen lächerlich machen, ist sogar verboten (es gilt das „Recht am eigenen Bild")! Frag immer die Abgebildeten vor dem Posten, ob sie damit einverstanden sind.

Apps sicher nutzen.
Lade Apps nur aus den offiziellen App-Stores. Checke die Zugriffsberechtigungen und verzichte lieber auf Apps, die zu viele Berechtigungen verlangen. Installiere regelmäßig die Software-Updates und lösche Anwendungen, die du nicht mehr brauchst.

Gegen Cyber-Mobbing aktiv werden.
Cyber-Mobbing ist kein Spaß, sondern eine strafbare Handlung! Gemeint sind Beleidigungen, Belästigungen oder Drohungen über Internet und Handy, die das Leben der Betroffenen sehr stark beeinträchtigen können. Setze dich gegen Cyber-Mobbing zur Wehr und unterstütze Mobbing-Opfer: Sichere Beweise (z. B. Screenshots), blockiere und melde Täter*innen* in Sozialen Netzwerken und hol dir Hilfe bei Leuten, denen du vertraust. Je früher, desto besser!
Auch Rat auf Draht (147) hilft dir weiter.

Umsonst gibt's nichts.
Auch im Internet ist selten etwas wirklich kostenlos. Sei bei „Gratis"- oder „Schnäppchen"-Angeboten stets misstrauisch, besonders wenn du dich mit Namen und Adresse registrieren oder das Angebot mit deinen Freund*innen* teilen musst. Meist sind die Anbietenden nur hinter deinen Daten her oder hinter dem „tollem" Angebot versteckt sich Schadsoftware. Auch Online-Gewinnspiele sind manchmal unseriös. Vorsicht, wenn die Preise allzu verlockend sind!

Computer & Handy schützen.
Verwende auf deinem Computer, Smartphone oder Tablet ein Anti-Viren-Programm und aktualisiere es regelmäßig. Bring auch laufend deine Software und Apps auf den aktuellsten Stand, am besten per automatischem Update. Schütze dein Gerät mittels PIN-Code, Passwort oder Entsperrmuster vor Zugriff durch Fremde!

Urheberrechte beachten.
Es ist in aller Regel verboten, Bilder, Musik oder Videos herunterzuladen und ohne Erlaubnis vom Rechteinhaber weiterzuverwenden. Verstöße gegen das Urheberrecht können richtig teuer werden!

Nicht alles im Internet ist wahr.
Sei misstrauisch! Vor allem besonders schockierende oder sensationelle Nachrichten sind oft gar nicht wahr. Manchmal werden absichtlich Gerüchte und falsche Geschichten verbreitet, um andere schlecht zu machen. Überprüfe Infos daher besser mehrfach – vergleiche zum Beispiel mehrere Quellen.

Kettenbriefe löschen.
Gruselige Nachrichten oder Kettenbriefe, die du an möglichst viele Freunde schicken sollst, lösen Angst oder sozialen Druck aus. Kettenbriefe sind frei erfunden. Schicke sie daher nicht weiter sondern lösche sie. Es ist völlig okay und gut, die Kette zu unterbrechen und nicht mitzumachen!
Klicke außerdem auf keine Links, diese können Schadsoftware enthalten.

Mehr erfahren:
www.saferinternet.at

HANDY ABER SICHER!

Sicherheitstipps für dein Handy

Stelle dein Handy so ein, dass du nach jedem **Neustart** deine SIM-Karten-PIN eingeben musst.

Sichere das Display mit einem **Sperrmuster** oder noch besser mit einem Passwort, Fingerabdruck oder Gesichtsscan (Biometrie).

Bewahre deine **PIN**, deinen PUK und dein Kundenkennwort sicher auf und speichere sie niemals direkt auf deinem Handy.

Achte darauf, dass deine Apps und dein Betriebssystem immer aktuell sind. Mache die **Software-Updates**.

Schalte **Bluetooth**, **GPS** und **WLAN** aus, wenn du sie nicht brauchst.

Lade Apps nur aus **offiziellen Stores** herunter (z. B. Google Play Store oder App Store).

Prüfe genau, welche **Berechtigungen** die App benötigt! Eine Taschenlampe braucht z. B. keinen Zugriff auf deinen aktuellen Standort.

Nicht immer sind kostenlose Apps die beste Wahl. Manchmal lohnt es sich, ein paar Euro zu investieren (für mehr Datenschutz, weniger Werbung ...).

Lösche Apps, die du nicht mehr benötigst.

Sichere regelmäßig deine Handydaten z.B. am Computer oder mit **Backup**-Apps.

Viele weitere wertvolle Tipps und Infos für Kinder, Jugendliche und Erwachsene findest du auf **www.saferinternet.at**

Rat auf Draht: Notruf für Kinder und Jugendliche – rund um die Uhr, anonym und kostenlos. Per Telefon (einfach **147** wählen), Onlineberatung oder Chat: **www.rataufdraht.at**

TIPPS FÜR ELTERN

Entdecken Sie das Internet **gemeinsam** mit Ihrem Kind. Suchen Sie interessante und spannende Websites, die dem Alter des Kindes entsprechen.

Einigen Sie sich auf **Regeln** zur Internet- und Handynutzung. z.B. den zeitlichen Umfang, die genutzten Inhalte, den Umgang mit Bildern oder die Kosten.

Sprechen Sie mit Ihrem Kind über die **Risiken** einer leichtfertigen Weitergabe von persönlichen Daten im Internet.

Vorsicht bei Treffen mit Online-Bekanntschaften! Nur an öffentlichen Orten und in Begleitung von Erwachsenen.

Diskutieren Sie den **Wahrheitsgehalt** von Online-Inhalten. Zeigen Sie Ihrem Kind, wie man Inhalte im Internet auf ihre Richtigkeit überprüfen kann, indem man andere Quellen zum Vergleich heranzieht. Auch Werbung ist für Kinder oft nur schwer zu durchschauen.

Schauen Sie nicht weg! Melden Sie kinderpornografische oder rechtsradikale Inhalte.
z.B. an www.stopline.at.

Auch im Internet gibt es **Regeln:** Was im realen Leben verboten ist, ist auch im Internet verboten.

Lassen Sie sich von Ihrem Kind aktuelle Lieblingsseiten, -spiele oder -apps zeigen und versuchen Sie zu verstehen, warum es diese toll findet.

Seien Sie nicht zu kritisch mit Ihrem Kind. Es kann durch Zufall auf ungeeignete Inhalte stoßen. Nehmen Sie dies zum Anlass, um über diese Inhalte zu diskutieren und Regeln zu vereinbaren.

Die Chancen digitaler Medien übertreffen die Risiken!
Unter Anleitung können die Risiken gut eingeschränkt werden.

Unter **www.saferinternet.at/zielgruppen/eltern** finden Sie weitere Informationen und konkrete Tipps:

WAS IST DAS EIGENTLICH?

MALWARE ist Schadsoftware wie Viren, Trojaner, Würmer oder Spyware, die darauf abzielt, Systeme zu beschädigen, Daten zu stehlen oder unbefugt Kontrolle zu erlangen.

FIREWALL ist ein Sicherheitssystem, das den Datenverkehr zwischen Netzwerken überwacht und unerwünschte oder gefährliche Verbindungen blockiert. Wie eine Schutzmauer.

AUTHENTIFIZIERUNG stellt sicher, dass eine Person oder ein System wirklich diejenige Identität besitzt, die sie vorgibt zu sein, z. B. durch Passwörter, Tokens oder biometrische Merkmale.

SOCIAL ENGINEERING bezeichnet Angriffe, die weniger auf Technik als auf menschliche Schwächen setzen, z.B. durch Manipulation, Täuschung oder Ausnutzen von Vertrauen.

MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA) erhöht die Sicherheit, indem mindestens zwei verschiedene Faktoren kombiniert werden, bevor Zugriff gewährt wird. Etwa Passwort und Smartphone-Code. Oft werden verschiedene Typen von Faktoren kombiniert: Etwas, das man *ist* (Biometrie) + etwas, das man *weiß* (Passwort) + etwas, das man *hat* (Smartphone)

VERSCHLÜSSELUNG (ENCRYPTION) schützt Daten, indem sie lesbare Informationen in eine für Unbefugte unverständliche Form umwandelt, die nur mit einem passenden Schlüssel entschlüsselt werden können.

PASSWORT-TRICKS 2

TIPPS FÜR EIN GUTES PASSWORT

Passwörter sollen möglichst lang und zufällig sein und für jeden Account neu gewählt werden, das weißt du bereits.

Hier findest du noch weitere Tipps für ein gutes Passwort.

01 **Lange und schwer zu erraten**
Ein Passwort sollte aus mindestens 16 Zeichen bestehen. Auch Sonderzeichen (!, ?, $...) sollten enthalten sein. Idealerweise kannst du einen Passwortgenerator verwenden.

02 **Nutz einen Passwort-Safe**
Damit du dir nicht alle Passwörter merken musst, kannst du einen Passwort-Safe benutzen. Dann musst du dir nur ein Passwort merken, das für den Safe! z.B. Keepass, 1Password

03 **Nutz die Zwei-Faktor-Authentifizierung**
Die Zwei-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsmaßnahme: Zusätzlich zum Passwort musst du beim Login eine weitere Sicherheitskomponente eingeben z.B. einen Pin-Code, den du per SMS bekommst.

04 **Speichere deine Passwörter nicht im Browser**
Wird das Browser-Konto gehackt, bekommt die Person gleich *alle* Passwörter auf einmal. Auch andere Personen, die das Gerät nutzen, können sie sehen.

Mehr Informationen:
www.watchlist-internet.at

WIE WERDEN PASSWÖRTER GEKNACKT?

**Jedes Passwort kann irgendwann geknackt werden.
Entscheidend ist, wie lange es dauert und wie aufwändig es ist.
Hier erfährst du, wie Angreifende vorgehen.**

„OFFLINE-CRACKING"

01 Daten stehlen:
Bei jedem Online-Dienst (E-Mail-Account, Online-Spiele, Social-Media...) legst du ein passwortgeschütztes Benutzerkonto an. Angreifer können diese Daten vom Server des Anbieters stehlen.

Aber: Die Passwörter werden nicht in Klartext gespeichert, sondern als Hash verschlüsselt. Ein Hash verschleiert dein Passwort und macht mit Hilfe von Mathematik eine Zahlen-/Buchstabenfolge daraus.

02 Entschlüsseln:
Hat ein Angreifer deinen Hash erbeutet, dann muss er/sie ihn noch entschlüsseln. Als Beispiel zeigen wir zwei gängige Methoden:

Brute-Force-Attack
Für jede Stelle des Passwortes wird jeder mögliche Buchstabe, Zahl oder Sonderzeichen ausprobiert. Je länger dein Passwort ist, desto mehr Möglichkeiten müssen die Angreifer berücksichtigen und brauchen dafür länger, um das Passwort zu knacken.

Dictionary-Attack
Mit einer Brute-Force-Attacke dauert die Berechnung der Passwörter eine Weile. Daher nehmen sich Hacker Wörterbücher oder Lexika zur Hand und probieren alle bekannten Begriffe aus, die dort enthalten sind. Nutzt du also ein Wort aus einem Wörterbuch, so kann ein Angreifer dein Passwort innerhalb von Minuten knacken. Auch Wörter von Internetseiten oder persönliche Informationen (Wohnort, Geburtsdatum,...) werden verwendet.

PASSWÖRTER STEHLEN

Häufig „verlieren" Benutzer*innen* selbst ihre Passwörter.

01 Soziale Manipulation/Phishing
Bei dir sollten die Alarmglocken läuten, wenn dir Unbekannte, Unternehmen oder Freunde einen komischen Link schicken oder nach deinem Passwort fragen. Absender von E-Mails können leicht gefälscht werden. Über die echt wirkende E-Mail wirst du auf eine gefälschte Webseite gelockt, die z.B. wie die Anmeldeseite deiner Bank aussieht.
Hier darfst du niemals deine Anmeldedaten eingeben!
Ob per E-Mail oder am Telefon: traue keinem, der einfach so nach deinem Passwort fragt!

02 Malware/Schadprogramme
Das ist ein Programm, das dir unbemerkt Schaden zufügt oder Daten stehlen kann. Häufig installieren sich Schadprogramme durch das unvorsichtige Surfen im Internet. Einige dieser Schadprogramme können deine Passwörter auslesen und sich ungebremst auf deinen Konten und Geräten bewegen. Deine Passwörter werden dann an Angreifende verschickt, ohne, dass du es bemerkst. Lade deshalb Software nur auf vertrauenswürdigen Seiten herunter und aktualisiere laufend deinen Virenschutz auf dem Computer und auf dem Smartphone.

03 Schulterblick-Methode
Das ist die einfachste und häufigste Methode in deinem Umfeld. Ein Freund hat dir beim Eingeben deines Passworts über die Schulter geschaut oder du hast dein Passwort zum Beispiel auf einem Notizblatt an den Computer-Bildschirm geklebt. Ähnlich ist das auch mit der Bildschirmsperre auf deinem Smartphone. Benutzt du dazu ein Muster, das du nachzeichnen musst, dann ist das oft sehr leicht zu durchschauen.

Quelle: https://mecodia-medienkompetenz.de/materialien/wie-werden-passwoerter-geknackt/

GARTENZAUN-VERSCHLÜSSELUNG

TRANSPOSITION

01 Klartext vorbereiten:
Entferne alle Leerzeichen und Satzzeichen.
Forschen mit Nori. → FORSCHENMITNORI
= 15 Zeichen

02 Entscheide, wie viele Zeilen du verwenden möchtest. 2-5 sind gut. In unserem Beispiel verwenden wir 3 Zeilen.

03 Verschlüsseln:
Zeichne dir eine Tabelle. Zeilen sind die von dir gewählte Zeilenanzahl. Die Anzahl der Spalten ergibt sich aus deinem Klartext. Bei uns sind es 15 Zeichen, also hat die Tabelle 15 Spalten.

04 Schreibe die Buchstaben jetzt im Zick-Zack-Muster in die Tabelle. Rechts siehst du das Beispiel.

Zum Abschluss schreibst du die Buchstaben auf, die in den Zeilen nacheinander stehen.

Forschen mit Nori → F C M O O S H N I N R R E T I

05 Zum Entschlüsseln brauchst du das Wort und die Anzahl der Zeilen (3). Zeichne die Tabelle und zeichne dir in der Tabelle das Zick-Zack-Muster vor. Jetzt trägst du die Buchstaben ein und zwar Zeile für Zeile (siehe rechts).

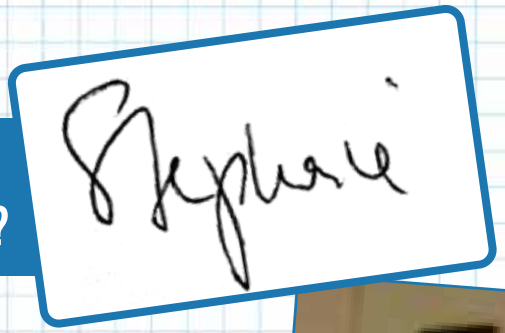
F				C				M				O		
	O		S		H		N		I		N		R	
		R				E				T				I

WIESO?

Die Gartenzaunverschlüsselung ist eine klassische **Transpositionschiffre**, bei der die Buchstaben nicht verändert, sondern in einer Zickzack-Struktur neu angeordnet werden. Dadurch entsteht ein Muster, das an einen Gartenzaun erinnert. Diese Methode gab es schon in der Antike.

Transposition ist ein wichtiger Bestandteil moderner Algorithmen. Die Gartenzaunverschlüsselung selbst wird aber hoffentlich nirgendwo mehr eingesetzt, sie ist viel zu leicht mit Computern zu knacken.

WORAN FORSCHST DU?



Ich forsche daran, wie man Cybersicherheit so erklären kann, dass sie für alle Menschen verständlich und spannend ist. Egal ob für Firmen oder junge Menschen.

Dabei ist mir besonders wichtig, dass sich Mädchen sicherer im Internet bewegen können und die Tricks von Angreifern erkennen.

DAS BIN ICH

Hier arbeite ich:
SBA Research

Hier bin ich in die Schule gegangen:
HLW Tulln

Das studiere ich:
Software Engineering und Information Security Management

Das wollte ich als Kind werden:
Architektin

Darum bin ich Forscherin geworden:

Weil mich Rätsel und Puzzle immer schon interessiert haben. Forschen ist wie Rätsel und Puzzle bauen in einem.

So bin ich auf die Idee zu meiner Forschung gekommen:

Ich hatte viele Gespräche mit Frauen, die Interesse an Cybersicherheit hatten, aber nicht wussten wo sie anfangen sollen hinein zu schnuppern. Zusätzlich hörte ich in der IT immer wieder, dass es doch so wenig Frauen in der Cybersicherheit gibt.

Deshalb habe ich **Shecurity** gegründet. Ich wollte die Sicherheitsexpertinnen zusammen bringen und verstehen was sie an dem Bereich interessiert und auch warum Mädchen und Frauen trotzdem keine Cybersicherheitsausbildung auswählen.

So sieht mein Alltag aus:

Jeder Tag sieht anders aus. Manche sind sehr voll mit Meetings, viele Gespräche und Mails.
Andere Tage bestehen aus Planung von Vorträgen und Trainings. Zwischendurch verarbeite und analysiere ich Gespräche und Daten zum Thema Cybersicherheit.

Sehr oft halte ich Vorträge für Frauen und zeige ihnen die Vielfalt der Cybersicherheit oder leite Arbeitsgruppen und Sitzungen.

Stefanie Jakoubi ist eine österreichische Expertin für Cybersecurity und Mitglied der Geschäftsleitung von SBA Research, einem österreichischen Forschungszentrum für Informationssicherheit.

Sie ist Gründerin der Initiative **Shecurity**, die Frauen den Einstieg in die IT-Sicherheit erleichtert und Diversität in der Branche stärkt. Als Obfrau der **Cyber Sicherheits Plattform** (CSP), wirkt sie an der Gestaltung der österreichischen Cybersecurity-Landschaft mit.

Außerdem ist sie Initiatorin des **Future IT Day**, der junge Menschen für IT begeistern soll. (shedigital.at/die-it-tag/).

Das soll meine Forschung bewirken:

Meine Forschung soll Mut machen. Mut für mehr Sicherheit im Internet und Mut seinen Weg in der Cybersicherheit zu finden.

So forsche ich genau:

Ich spreche mit vielen Expert*innen* über Cybersicherheit, Ausbildung, Rollenbilder und auch mit Frauen, die in der IT arbeiten und mit denen die Interesse an Cybersecurity haben.

Mit all diesen Informationen versuche ich, Angebote zum Einstieg in die Cybersicherheit zu entwickeln.

Das mache ich in meiner Arbeit am liebsten:

Mädchen und Frauen einen Einblick in die Cybersicherheit zu geben und ihnen einen Weg zu zeigen.

Das fand ich bisher am schwierigsten:

Zu viele Forschungsideen auf einmal zu haben.

Darüber habe ich mich in meiner Arbeit bisher am meisten gefreut:

Zu sehen, welche Auswirkungen meine Arbeit hat.
Frauen, die bei einem unserer Formate zum ersten Mal mit Cybersicherheit in Kontakt gekommen sind und Interesse überschwappte. Sie merkten, dass dieses Feld nicht so unzugänglich ist, wie es von außen oft wirkt. Wenn mir Teilnehmerinnen nach einigen Workshops erzählen, dass Sie sich für eine Security Rolle beworben haben, Cybersicherheit studieren oder sich getraut haben, in der Arbeit gelerntes Cybersicherheitswissen anzuwenden, freut mich das sehr.
Es zeigt mir wie wichtig meine Forschung ist.

Was würdest du mir raten, wenn ich auch Wissenschafter*in* werden will?

Höre nie auf neugierig zu sein.

BESUCH BEI

FABIAN FISCHER

INSTITUT FÜR TECHNIKFOLGENABSCHÄTZUNG
ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

IT-SECURITY

WARUM IT-SCHUTZ ZU HAUSE BEGINNT UND WIE ALTERSCHECKS OHNE DATENKLAU FUNKTIONIEREN KÖNNEN

Fabian Fischer vom Institut für Technikfolgenabschätzung (ITA) der Österreichischen Akademie der Wissenschaften beschäftigt sich damit, wie Technik unseren Alltag verändert. Im Gespräch erklärt er Lea von FÄKT, warum IT-Sicherheit heute zu Hause beginnt und wie eine faire Altersprüfung im Netz aussehen könnte, die unsere Privatsphäre nicht zerstört.

TECHNIKFOLGENFORSCHUNG
beschäftigt sich mit den Auswirkungen neuer Technologien auf Gesellschaft, Umwelt und Wirtschaft. Die Forschenden untersuchen unabhängig die Chancen und Risiken technischer Innovationen und bereiten dieses Wissen für Wirtschaft, Politik und Öffentlichkeit auf. Sie schaffen damit eine fundierte Grundlage für Entscheidungen, indem sie komplexe Auswirkungen neuer Technologien verständlich machen.

Zuhause fühlt man sich sicher, die Fenster sind geschlossen, die Türen und wichtigen Dokumente kann man versperren. Aber stellt euch vor, die Tür wäre offen, fremde Personen können in euren Familienalben schnüffeln oder eure Schreibtischladen durchwühlen und die Daten auf eurem Pass lesen. Ein ziemlich unangenehmes Gefühl, oder?

Im digitalen Raum passiert genau das leider oft, ohne dass wir es merken. Kreditkarten Details geleakt, die Ausweisdetails im Darknet verfügbar, der Internetbetrug kann beginnen.

FABIAN, DU ARBEITEST AM ITA. WAS GENAU UNTERSUCHST DU DORT ALS „TECHNIKFOLGEN-ABSCHÄTZER“?
Wir schauen uns neue Technologien an, idealerweise bevor sie überall im Einsatz sind, und fragen: Was macht das mit den Menschen und der Gesellschaft?

EIN RIESENTHEMA MOMENTAN IST DIE ALTERSVERIFIKATION, AUCH WEGEN DES SOCIAL MEDIA VERBOTS BIS 14 JAHRE. MÜSSEN WIR BALD ALLE UNSER GESICHT SCANNEN LASSEN, UM SOCIAL MEDIA ZU NUTZEN?
Das ist genau die Gratwanderung, die wir gerade untersuchen. Es gibt politischen Druck, das Alter im Netz strenger zu prüfen, um Kinder zu schützen. Aber unsere Frage ist: Wie stelle ich sicher, dass jemand alt genug ist, ohne dass die App sofort weiß, wer ich bin und Zugriff auf z.B. Ausweisdetails hat?

Momentan gibt es oft nur zwei Extreme: Entweder man kann beim Alter einfach schummeln oder man muss seinen Ausweis hochladen. Beides ist nicht ideal.
Wir am ITA suchen nach technischen Lösungen, die „Privacy-Preserving“ sind, also privatsphärenschonend.

WIE KÖNNTE SO EINE LÖSUNG KONKRET AUSSEHEN, OHNE DASS ICH ZUM „GLÄSERNEN USER“ WERDE?
Das Ziel ist eine Technik, die der Plattform nur ein „Ja“ oder „Nein“ übermittelt: „Ja, diese Person ist über 14“.

Lea vom FÄKT-Team besucht Fabian, der sich hier mit seinen Kolleg*innen* mit den Auswirkungen neuer Technologien auf Gesellschaft, Umwelt und Wirtschaft beschäftigt.

Die App erfährt aber weder deinen Namen noch dein Geburtsdatum oder wie du aussiehst. Wir konnten feststellen, dass glücklicherweise an solchen Lösungen gearbeitet wird, ohne unnötige sensible Daten an einen Server zu schicken.
Wir wollen eine Lösung, die Kinder schützt, ohne dass sie für jeden Login ihre gesamte Identität preisgeben müssen.

IT-SICHERHEIT KLINGT OFT NACH HACKER-ANGRIFFEN AUF BANKEN. WARUM BETRIFFT DAS EINE GANZ NORMALE FAMILIE IN ÖSTERREICH?

In einer typischen Familie hängen heute der Staubsaugroboter, Waschmaschine und die Spielkonsole im selben WLAN wie das Tablet für das Online-Banking. Oft sind diese kleinen Geräte schlecht gesichert, und im blödesten Fall erhalten sie keine Sicherheitsupdates – werden Lücken entdeckt, werden sie also nicht gestopft und Hacker haben leichtes Spiel. Wenn der Staubsaugerroboter gehackt wird, ist das wie ein offenes Fenster im Erdgeschoss: Der Einbrecher ist im Haus. IT-Sicherheit beginnt also beim Router im Flur.

WAS WÜRDEST DU FAMILIEN RATEN, UM DIE EIGENE SICHERHEIT IM DIGITALEN NETZ ZU SCHÜTZEN?

Ein ganz einfacher technischer Kniff: Nutzt für eure „smarten" Geräte wie den Staubsauger das Gast-WLAN eures Routers.
So trennt ihr die unsicheren Gadgets von euren privaten Handys.

Und: Nutzt die **Zwei-Faktor-Authentifizierung (2FA).** Das ist wie ein zweites Schloss an der Tür, selbst wenn jemand dein Passwort knackt, kommt er ohne den Code auf deinem Handy nicht rein.

Alte Geräte, die keine Sicherheitsupdates mehr bekommen, im besten Fall gar nicht mehr ins WLAN lassen.

Auch liebe Eltern - Keine Fotos von Kindern öffentlich ins Netz stellen! Ich rate Familien zu einem „Foto-Pakt": Gepostet wird nur, wenn alle auf dem Bild zustimmen. Das ist eine Form von Respekt, denn Jugendliche und Kinder sollten ihren Eltern ruhig sagen können: „Das ist meine Privatsphäre, frag mich bitte vorher."

TIPP:
Vereinbart einen Foto-Pakt: Keine Posts ohne Erlaubnis ***ALLER*** *Beteiligten (auch nicht durch die Eltern!).*

LUST AUF MEHR SCIENCE?

Spannende Science Videos findest du auf dem YouTube Kanal von FÄKT
@faekt.science

und in den sozialen Medien:
Instagram
TikTok
@faekt.science

Die **ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN** ist die größte Forschungsorganisation in Österreich, die nicht zu einer Universität gehört. Hier forschen rund 1000 Wissenschafter*innen* zu spannenden Themen.

FÄKT wurde ins Leben gerufen, um komplexe Forschungsthemen für Kinder und Jugendliche aufzubereiten. Die kurzen Science Videos haben auch im Schulunterricht Platz: zu jeder Folge gibt es Begleitmaterial für die SEK 1. Finanziert ist das Projekt durch den Fonds Zukunft Österreich. Für das ForscheN-Magazin besucht das FÄKT-Team Wissenschafter*innen* und erfährt Erstaunliches über deren Arbeit.

Nori und das große Geheimnis

Nori kennt das Rezept für einen Zaubertrank.
Es ist streng geheim.

Seine Freundin Lilli Biber möchte das Rezept unbedingt haben. Sie braucht den Zaubertrank ganz dringend sagt sie und verspricht, das Rezept niemals an niemanden weiterzugeben: „Ich verspreche, ich sag's niemandem weiter!"

Was könnte der Zaubertrank bewirken?

Nori möchte Lilli helfen, aber er weiß: Wenn das Rezept in die falschen Pfoten gelangt, ist das gar nicht gut!
Ein Zaubertrankrezept ist etwas Besonderes.
Angestrengt überlegt Nori: Soll er das Rezept teilen?

Was soll Nori tun?

Fast schon hätte Noris Kopf vom vielen Nachdenken zu rauchen begonnen, da beschließt er: „Ich kenne Lilli gut, ich vertraue ihr. Bei Lilli ist das Rezept sicher aufgehoben." Er kennt Lilli wirklich schon lange, sie spielen oft zusammen und er war auch schon bei ihrer Familie im Biberbau zu Hause. Noch nie hat sie ein Geheimnis weitererzählt.

Jetzt bleibt nur noch das Problem, dass Lilli seit kurzem sehr weit weg wohnt. Viel zu weit, dass Nori mit seinen Federflügelohren einfach zu ihr fliegen könnte.

Wie soll das Rezept zu Lilli kommen?

Lilli ist ein Biber und lebt in einem Biberbau. Sie schlägt vor, das Rezept in eine Flaschenpost zu stecken und den Bach abwärts zu ihr zu schicken. Weil die Biberburg den ganzen Bach absperrt, kann sie die Flaschenpost nicht verpassen. Doch was ist, wenn jemand anderes die Flaschenpost vor Lilli entdeckt?

Wie kann Nori das Rezept schützen?

Nori hat eine Idee! Er zeichnet ein Bild. Als er fertig ist, holt er einen kleinen Ast und sticht damit viele Löcher in das Bild. Sie sind wie Gucklöcher. Das Bild ist trotzdem noch schön.

Dann legt er ein zweites Blatt Papier darunter und schreibt in jedes der kleinen Löcher einen Buchstaben vom Zaubertrankrezept. Die Zeichnung ist wie eine Schablone. Als Nori fertig ist, hebt er die Zeichnung hoch. Auf dem Blatt sieht man jetzt die Buchstaben und Zahlen überall am Blatt verteilt. In die Zwischenräume schreibt Nori irgendwelche Buchstaben.

Nori ist ein Wiffzack, er schickt nicht beides gemeinsam weg, das wäre unvorsichtig. Zuerst kommt die Zeichnung mit den Löchern, die Lilli zum Entschlüsseln braucht, in eine erste Flaschenpost. Das Rezeptblatt versteckt Nori derweil sicher in seiner Höhle. Die Zeichnung rollt er zusammen, steckt sie in eine Flasche, verschließt sie gut und wirft sie in den Bach. Die erste Flaschenpost macht sich auf die Reise.

Hoch oben in den Bäumen flattert die Elster von Ast zu Ast. Ihre Augen funkeln vor Neugier. Sie liebt es, Sachen zu finden, die nicht für sie bestimmt sind. Besonders wertvolle Sachen. Oder geheime Sachen. Oder wertvolle geheime Sachen. Da wird sie auf die Flasche im Bach aufmerksam. „Oho, was haben wir denn da?“ krächzt sie. Sie zieht das Blatt aus der Flaschenpost, entrollt es und sieht… eine kaputte Zeichnung mit Löchern. „Seltsam. Aber nicht wertvoll und nicht geheim. Weg damit.“ Mit einem beleidigten Flügelschlag wurschtelt sie die Zeichnung wieder in die Flasche und wirft diese in den Bach zurück. Die Reise geht weiter.

Ein paar Tage später schickt Nori die zweite Flaschenpost weg. Diesmal mit dem verschlüsselten, streng geheimen Zaubertrankrezept.

Wieder entgeht der neugierigen Elster nichts und sie findet die Flaschenpost. Sie schaut sie an: „Was ist das für ein Gekritzel? Da kann wohl jemand noch nicht schreiben, tztztztz“. Auch diesmal steckt sie den Zettel zurück in die Flasche und wirft die Flaschenpost wieder in den Bach.

Wird das Geheimnis sicher bei Lilli ankommen?

Viel weiter flussabwärts versperrt die Biberburg von Lillis Familie den ganzen Bach. Zwischen zwei Ästen verfängt sich eine Flaschenpost. Lilli merkt sofort, dass da etwas für sie angekommen ist. Sie schwimmt hin und freut sich sehr. Als sie das Blatt mit den seltsamen Buchstaben und Zahlen sieht, weiß sie sofort, was zu tun ist.

Lilli holt die Zeichnung von Nori hervor. Die hat sie vor ein paar Tagen schon aus dem Bach gefischt. Jetzt legt sie vorsichtig das Blatt und die Zeichnung übereinander. „Was für ein gescheiter Nori du bist!“ denkt sich Lilli. In den Löchern der Zeichnung entdeckt sie genau die Buchstaben für das Rezept.

Viel weiter flussaufwärts baumelt unser Nori mit den Füßen. Er lächelt und insgeheim weiß er, dass seine streng geheime Nachricht sicher bei seiner Freundin angekommen ist.

BLITZ-EXPERIMENT

WIE SICHER IST MEIN PASSWORT?

1 Teste die Stärke von Passwörtern auf dieser Website:

https://checkdeinpasswort.de

2 Die Seite zeigt dir an, wie lange Hacker mit einem normalen PC ungefähr brauchen würden, um dein eingegebenes Passwort zu knacken.

Teste mit unterschiedlich langen Passwörtern. Benutze Zahlen und Sonderzeichen. Was verändert sich dadurch?

3 Aus Sicherheitsgründen solltest du **nicht** deine echten Passwörter eingeben!

Impressum:
Medieninhaber und Herausgeber: Land Niederösterreich, Amt der NÖ Landesregierung, Abteilung Wissenschaft und Forschung, Landhausplatz 1, 3109 St. Pölten, www.noe.gv.at/wissenschaft, forschen@noel.gv.at
Idee, Redaktion und Gestaltung: Abteilung Wissenschaft und Forschung, Christina Kuback | Redaktionsteam: in Kooperation mit Peter Kieseberg, Simon Tjoa (USTP) sowie Lea Pichler (OAW) | Bildnachweise: Experimente: Abteilung Wissenschaft und Forschung, Simone Weiß | Coverfoto sizsus, Weinfranz 2, Adobe Stock: Дмитрий Горелкин 4-7, 16-17, L.Bouvier 8, dzmitry 9, beginagain 14, ImageFlow 18, Thawatchai Images 19, Alberto Masnovo 30, Lea Pichler 30, Tunazzinaakhter 36, Nuno Mendes 37, AbdurRahman 38 | Druck: Amt der NÖ Landesregierung, Abt. Gebäudemanagement, Amtsdruckerei | Herstellungsort: St. Pölten | Datenschutz: Detaillierte Informationen zur Verarbeitung von Daten, zu den Rechten als betroffene Person sowie zum Beschwerderecht bei der Datenschutzbehörde sind im Internet unter www.noe.gv.at/datenschutz abrufbar. | Die in diesem Magazin dargestellten Experimente wurden sorgfältig von der Herausgeberin ausgesucht und geprüft. Die Herausgeberin kann jedoch nicht ausschließen, dass einzelne Experimente nicht in der dargestellten Weise gelingen. Die Haftung für das Gelingen der Experimente und mögliche Schäden bei ihrem Fehlschlagen wird, soweit gesetzlich zulässig, ausgeschlossen. | Ein diskriminierungsfreier, geschlechtersensibler Sprachgebrauch ist wesentlich für die Gleichbehandlung und Gleichstellung aller Geschlechter. Dieses Magazin richtet sich an alle Menschen, unabhängig von Geschlechtsidentität, Geschlechtsmerkmalen und Geschlechtsausdruck. | Das ForscheN-Magazin wird als Fachinformation der Abteilung Wissenschaft und Forschung kostenlos herausgegeben. Es ist nicht zum Verkauf bestimmt. Alle Angaben ohne Gewähr. Kein Anspruch auf Vollständigkeit.
Für etwaige Druckfehler wird keine Haftung übernommen. Für Hinweise, Ergänzungen und Korrekturen danken wir im Vorhinein.

DU WILLST MEHR FORSCHEN?

In Niederösterreich gibt es viele Angebote, bei denen du Wissenschaft und Forschung auf vielfältige Weise erleben kannst. Sowohl in der Freizeit als auch im schulischen Kontext. Das Angebot reicht von Vorträgen und Workshops bis hin zu Exkursionen und Lehrgängen.

Auch dein kostenloses Abonnement des ForscheN-Magazins kannst du hier bestellen. Ein kostenloses Klassenabonnement können Lehrkräfte über forschen@noel.gv.at bestellen.

sciencecenter.noe.gv.at/wissenschafterleben