Schutz persönlicher Daten

Man sollte sich gut überlegen, welche Daten man im Internet über sich selbst teilt und auch wo genau man sie preisgibt. Kommen individuelle Informationen nämlich in die falschen Hände, kann es zu **Missbrauch der Daten** kommen, wie zum Beispiel zum Identitätsklau. Darum ist es wichtig auf die persönlichen Informationen aufzupassen. Oft sind zum Beispiel Online-Services an unseren Daten interessiert, um aufgrund unserer „Likes" zu sehen was unsere Interessen sind. Diese Informationen erleichtern es den Konzernen personalisierte **Werbung** zu schicken, um mehr Gewinn zu machen. Das Problem daran ist: Je mehr Informationen wir online über uns preisgeben, desto genauer und zielgerichteter kann Werbung für uns gestaltet werden.

Zusätzlich darf nicht vergessen werden, dass Daten, die frei im Netz zugänglich sind, von jedem eingesehen und auch zurückverfolgt werden können. Darum sollte man nicht nur darauf achten, welche Informationen man online gibt, sondern auch welche Fotos man postet, wenn man nicht möchte, dass diese von jedem Menschen gesehen werden können.

Daten sind sehr vielfältig: Sie reichen von **privaten Daten**, wie Name und Adresse (=schutzbedürftige Daten), über weniger persönliche Angaben, wie das Lieblingsgericht oder die Lieblingsfarbe. Das Lieblingsgericht sagt nichts Spezifisches über eine Person aus und kann daher kaum missbräuchlich verwendet werden. Es ist aber schon problematisch, wenn eine fremde Person Zugriff auf den Namen und die Adresse hat, da es hierbei zu Identitätsklau oder anderem Datenmissbrauch kommen kann. Einem besonderen Schutz unterliegen die **sensiblen Daten**. Dazu gehören Informationen über die Gesundheit, die politische Einstellung, oder religiöse oder philosophische Überzeugungen. Diese Informationen sind sehr persönlich und sollten nicht in den öffentlichen Umlauf geraten.

Um im Internet möglichst sicher mit Daten umzugehen, könnten folgende Tipps helfen:

- Bei Registrierungen sollten **Nicknames anstatt echter Namen** benutzt werden.
- Die **Privatsphäre-Einstellungen auf sozialen Netzwerken**, oder auf Plattformen, auf denen man registriert ist, sollten immer wieder überprüft und gegebenenfalls geändert werden.
- Es sollte immer hinterfragt werden, **ob und wann es sinnvoll ist**, schutzbedürftige Daten anzugeben. Bestelle ich zum Beispiel ein Geschenk, macht es Sinn, die Adresse anzugeben, damit der/die Postausträger:in weiß, wohin das Paket geliefert werden muss. Fragt aber eine Spiele-App nach meiner Wohnadresse, ist dies sehr kritisch, da es keinen guten Grund gibt, wieso diese Information von der App benötigt wird.
- E-Mails, die **unbekannt sind oder fragwürdige Anhänge beinhalten**, sollten nicht aufgemacht werden. Dahinter könnte sich zum Beispiel eine Spionage-Software befinden, die die persönlichen Daten ausliest.
- Passwörter sollten sehr **sicher und geheim** gehalten sein.
- Für Registrierungen kann eine **zweite Email-Adresse** angelegt werden, die nicht den eigenen Namen verwendet.

Passwörter

Ein Passwort ist vergleichbar mit einem Hausschlüssel: Wir benutzen diesen, um unsere Türe auf- und zu zusperren, da wir nicht wollen, dass eine fremde Person einfach so in unsere privaten Räumlichkeiten eintritt und sich persönliche Dinge ansieht oder sogar stiehlt. Der Schlüssel zu unserer Privatsphäre bleibt also bei uns. Das funktioniert in der digitalen Umgebung sehr ähnlich: Ein Passwort kann man als digitalen Schlüssel verstehen, mit welchem man auf Dinge, wie Accounts, WLAN oder Konten zugreifen kann.

Unabhängig davon, für welchen Zugang sie verwendet werden, sind Passwörter äußerst wichtig, um im Internet sicher zu sein und nur selbst auf die eigenen Inhalte Zugriff haben zu können. Jedoch bietet nicht jedes Passwort einen sicheren Schutz: „Hallo“ oder „123“ sind zwar immer noch beliebt und einfach zu merken, sind aber für andere leicht zu erraten. Konten oder Accounts können so leicht gehackt werden und für fremde Personen ersichtlich sein. Daher ist es sehr wichtig, dass Passwörter gewählt werden, welche für außenstehende Menschen schwer nachvollziehbar sind.

Um ein sicheres Passwort zu kreieren, sollte auf folgende Punkte geachtet werden:

- Das Passwort sollte **nicht zu kurz** sein. Mindestens 8-10 Zeichen sind optimal, um es nicht so leicht knacken zu können.
- Als Passwort sollten **keine logischen Folgen**, wie „1234“, oder Namen von Familienmitgliedern oder Haustieren verwendet werden. Solche Passwörter sind zu leicht zu erraten.
- **Je komplexer ein Passwort ist, desto sicherer ist es**. Es sollten also Groß- und Kleinschreibung sowie Sonderzeichen und Zahlen verwendet werden.
- Das Passwort darf **auf keinen Fall weitergesagt** werden.
- Wird ein Passwort aufbewahrt, darf dieses **nie als unverschlüsselte Datei** auf PC, Tablet oder Smartphone abgespeichert werden. Auch aufgeschrieben auf einem Zettel in der Nähe des Computers hat ein Passwort nichts verloren. Stattdessen sollte ein Passwort-Manager verwendet werden.
- Die **Zwei-Faktoren-Authentifizierung** bietet doppelte Sicherheit, um den Zugang auf Konten für andere so verschlüsselt wie möglich zu halten. Hierbei wird zusätzlich zur Eingabe des Passwortes ein Zahlencode angefordert.

Verschlüsselung

Ein Weg, um in der digitalen Welt sicher mit Daten umzugehen, ist die Verschlüsselung. Durch diese Methode können sensible Informationen in eine Art **geheimen Text** umgewandelt werden, der nur mit einem geheimen Schlüssel geöffnet werden kann. So funktionieren zum Beispiel viele Chats: Wenn man jemandem eine digitale Nachricht senden möchte, dann ist es wichtig, dass diese Nachricht nur von der Person gelesen wird, an die sie auch gerichtet ist. Das verhindert, dass äußere Quellen mitlesen können und eventuell sogar intime Informationen gesammelt werden.

Damit das nicht passiert, braucht man einen Weg, um den zu vermittelnden Text für andere unzugänglich zu machen. Das wird zum Beispiel durch eine **Ende-zu-Ende Verschlüsselung** ermöglicht, worüber viele Anbieter, wie z.B. Signal, verfügen. Das bedeutet, dass beim Herunterladen der App ein **Code** (also ein Schlüssel) auf dem eigenen Endgerät erstellt wird, der nicht von Anderen, nicht einmal von der App selbst, eingesehen werden kann. Beim Senden einer Nachricht wird dann genau dieser Schlüssel benutzt, um die geschriebene Nachricht unlesbar zu machen. Wählt man nun eine:n Empfänger:in für diese spezifische Nachricht aus, kann diese Person die Nachricht mit einem eigenen Schlüssel wieder lesbar machen. Somit kann der Text nur von dem/der Sender:in und dem/der Empfänger:in gelesen werden. Das soll eine sichere digitale Kommunikation gewährleisten.

Verschlüsselung funktioniert natürlich bei allen möglichen Dingen, wie zum Beispiel Dateien, Inhalten von Datenträgern oder eben Nachrichten. Kurz gesagt kann man sich Verschlüsselung wie einen Safe vorstellen, auf dessen Inhalte man nur mit einem bestimmten Code zugreifen kann.

Verschlüsselungsmöglichkeiten gibt es übrigens schon sehr lange: **Julius Cäsar** zum Beispiel verschob alle Buchstaben im Alphabet um zwei Zeichen, um so geheime Nachrichten zu verschicken. Nur die Personen, die über die Verschlüsselung Bescheid wussten, konnten die Botschaft also entziffern. Diese Methode wurde später durch die Chiffrierscheibe vereinfacht. Ob auch ihr diese für die Entschlüsselung des Lösungswortes nutzen könnt?

Recherchieren und Falschmeldungen erkennen

Uns alle erreichen jeden Tag unzählige Informationen - über unsere Social Media Apps, über Webseiten, Fernsehen, Zeitungen … Leider stimmen viele dieser „Informationen“ nicht. Bewusst gestreute Falschinformationen, die sich besonders schnell über soziale Netzwerke verbreiten, werden "Fake News" genannt. Sie sind gefährlich, weil Menschen ihr Verhalten an diesen Informationen ausrichten und falsche Entscheidungen treffen können.

Oft ist es gar nicht so einfach, Fake News zu erkennen.

Einige Fragen helfen dabei:

- **Ist der Inhalt logisch nachvollziehbar?**
  Passen alle Informationen in dem Artikel oder Video zusammen? Ist alles logisch erklärbar?
- **Ist der Stil sachlich oder emotional?**
  Wenn ein Text, Bild oder Video besonders unsere Gefühle anspricht, ist das ein Hinweis, dass wir damit beeinflusst werden sollen.
- **Über welchen Kanal, welche Person oder Webseite wurde die Information veröffentlicht? Ist diese Quelle seriös?**
  Stammt die Information von einer Nachrichtenseite oder einer seriösen Zeitung, kann man ihr eher vertrauen als dem Posting einer Einzelperson oder einem Artikel in einer Gratiszeitung.
- **Wer hat den Text geschrieben? Ist der/die Autor:in qualifiziert, zu diesem Thema etwas zu sagen? Gibt es überhaupt eine:n feststellbare:n Autor:in?**
  Wenn gar kein:e Autor:in aufgeführt ist, ist grundsätzlich Misstrauen angesagt. Ansonsten sollte geprüft werden, ob der oder die Autor:in sich in dem betroffenen Fachbereich auskennt.
- **Welches Interesse könnte dahinter stecken?**
  Hinter spektakulären Meldungen steckt oft das Interesse, dass sie sich möglichst schnell verbreiten und die damit verbundene Werbung viele Menschen erreicht.
- **Ist diese Information auch in anderen Quellen zu finden?**
  Wenn Informationen in mehreren - seriösen - Kanälen zu finden sind, ist das ein Hinweis, dass sie tatsächlich wahr sind.
- **Werden nachprüfbare Daten und Fakten genannt?**
  Wenn in einem Artikel oder Video viele Andeutungen gemacht, Fragen gestellt und Verdächtigungen in den Raum gestellt werden, ist das wenig glaubwürdig. Werden dagegen klare Zahlen, Daten und Fakten genannt, ist es wahrscheinlicher, dass die Information stimmt.
- **Bezieht sich der Inhalt auf andere Quellen? Wenn ja, welche, seriös oder nicht?** Wenn in einem Beitrag auf andere Quellen verwiesen wird, ist das ein Hinweis auf den Wahrheitsgehalt, aber auch diese anderen Quellen müssen auf Seriosität geprüft werden.