2020-1-DE02-KA227-ADU-008321

Co-funded by the
Erasmus+ Programme
of the European Union

Broschüre

Zur Verwendung von ICT-Tools

Erstellt von den Partnern des
Projektes "DIGITALIZE - Werkzeuge für erwachsene Roma
zur Nutzung des Internets und zur Förderung der Bildung"

Partner-Organisationen:

Amaro Foro e.V.

EGYÜTT HATÓ
KÖZÖSSÉGÉPÍTŐ EGYESÜLET

NEVO PARUDIMOS

ROMA

- Meine Broschüre zur Verwendung von IKT-Werkzeugen -

Projekt "Digitalize - tools for Roma adults to use the internet and promote education"

Dieses Dokument wurde im Rahmen des Projektes "Digitalize - tools for Roma adults to use the internet and promote education" erstellt, das von Amaro Foro e.V., Együttható Egyesület, Nevo Parudimos und RROMA durchgeführt wird. Das Projekt wird durch das Erasmus+ Programm der Europäischen Union unterstützt. Projektnummer: 2020-1-DE02-KA227-ADU-008321. Die Unterstützung der Europäischen Kommission für die Erstellung dieser Publikation stellt keine Billigung des Inhalts dar, der ausschließlich die Ansichten der Autoren wiedergibt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.

Verfasser: YOZKAN, Pelin - Együttható Egyesület

Co-funded by the Erasmus+ Programme of the European Union

- Inhaltsübersicht -

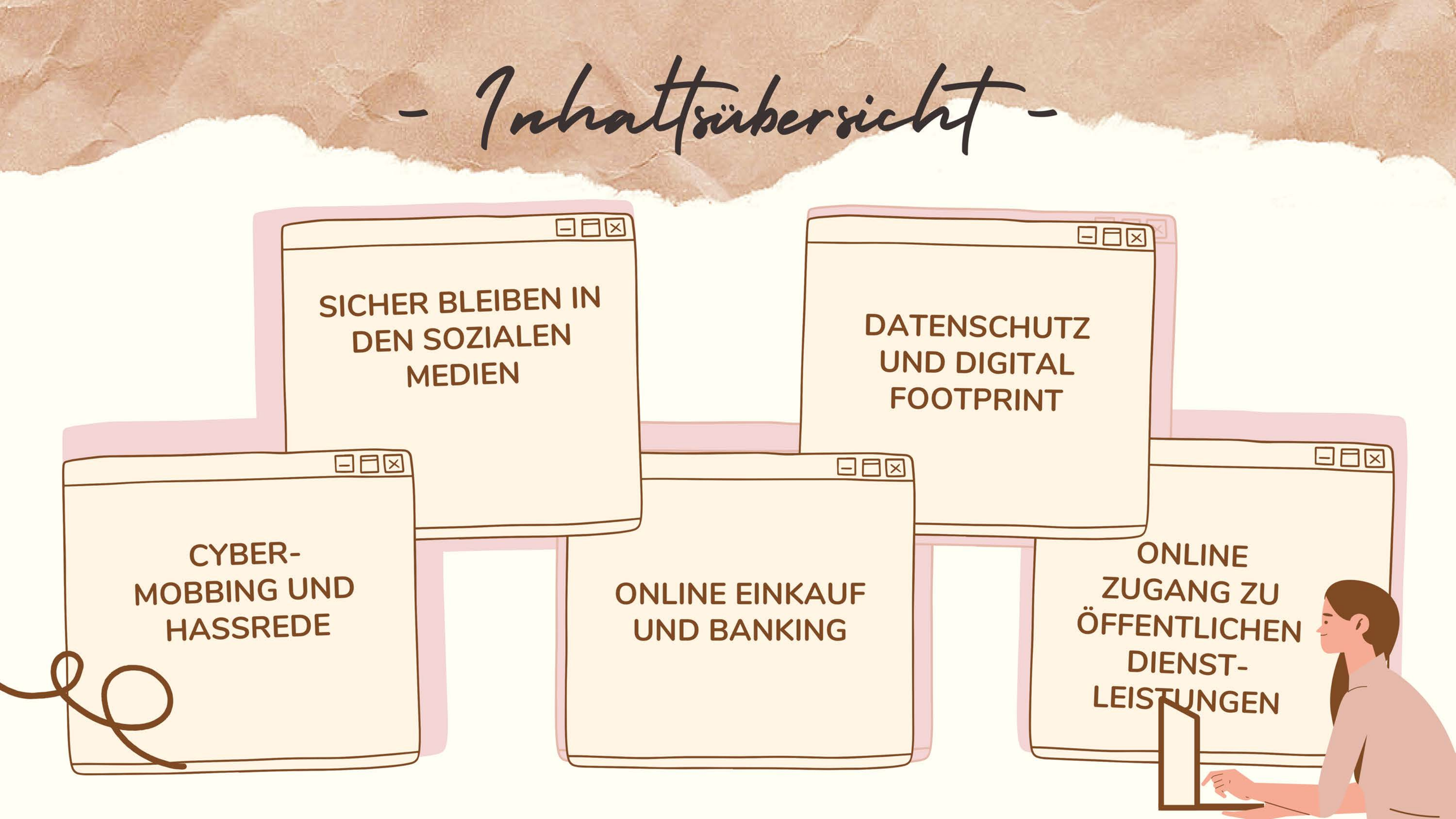
SICHER BLEIBEN IN DEN SOZIALEN MEDIEN

DATENSCHUTZ UND DIGITAL FOOTPRINT

CYBER-MOBBING UND HASSREDE

ONLINE EINKAUF UND BANKING

ONLINE ZUGANG ZU ÖFFENTLICHEN DIENST-LEISTUNGEN



Hier sind unsere 10 besten Tipps, um in den sozialen Medien sicher zu bleiben:

Tip 1

Verwenden Sie ein sicheres Passwort

Machen Sie Ihre Passwörter einzigartig!

Verwenden Sie für jedes Ihrer Online-Konten ein anderes Passwort. Die Wiederverwendung von Passwörtern ist riskant!

Facebook Instagram Tiktok Bank account

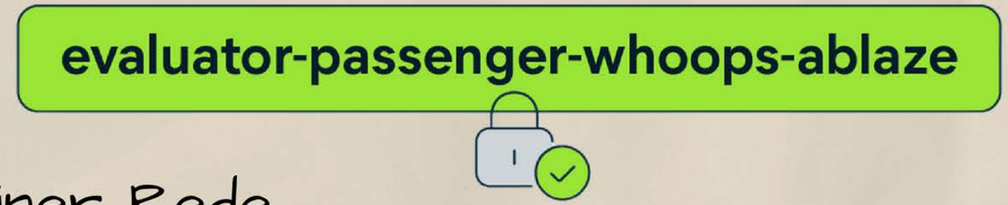
Wenn jemand Ihr Passwort für ein Konto in die Hände bekommt, kann er auf Ihre E-Mail, Ihre Adresse und sogar auf Ihr Geld zugreifen.

Tip 1

Verwenden Sie ein sicheres Passwort

Machen Sie Ihr Passwort länger und einprägsamer!

Lange Kennwörter sind sicherer, daher sollte Ihr Kennwort mindestens 12 Zeichen lang sein.



Versuchen Sie zu verwenden:

- Ein Text aus einem Lied oder Gedicht
- Ein bedeutungsvolles Zitat aus einem Film oder einer Rede
- Eine Reihe von Wörtern, die für Sie von Bedeutung sind
- Eine Abkürzung: Bilden Sie ein Passwort aus dem ersten Buchstaben eines jeden Wortes in einem Satz.

Tip 1

Verwenden Sie ein sicheres Passwort

Vermeiden Sie persönliche Informationen und allgemeine Wörter!

Erstellen Sie keine Passwörter aus Informationen, die andere kennen oder leicht herausfinden könnten (wie die zugänglichen Informationen in Ihrem Social-Media-Profil).

Zum Beispiel,

- Ihr Spitzname oder Ihre Initialen
- Der Name Ihres Kindes oder Haustiers
- Wichtige Geburtstage oder Jahreszahlen
- Der Name Ihrer Straße
- Zahlen aus Ihrer Adresse

Tip 1 Verwenden Sie ein sicheres Passwort

Verwenden Sie keine gewöhnlichen, einfachen Wörter, Phrasen und Muster, die leicht zu erraten sind!

Beispiele:

- Offensichtliche Wörter und Ausdrücke wie "Passwort" oder "IhrName"
- Sequenzen wie "abcd" oder "1234"
- Tastaturmuster wie "qwerty" oder "qazwsx".

Tip 1

Verwenden Sie ein sicheres Passwort

Bewahren Sie Passwörter sicher auf!

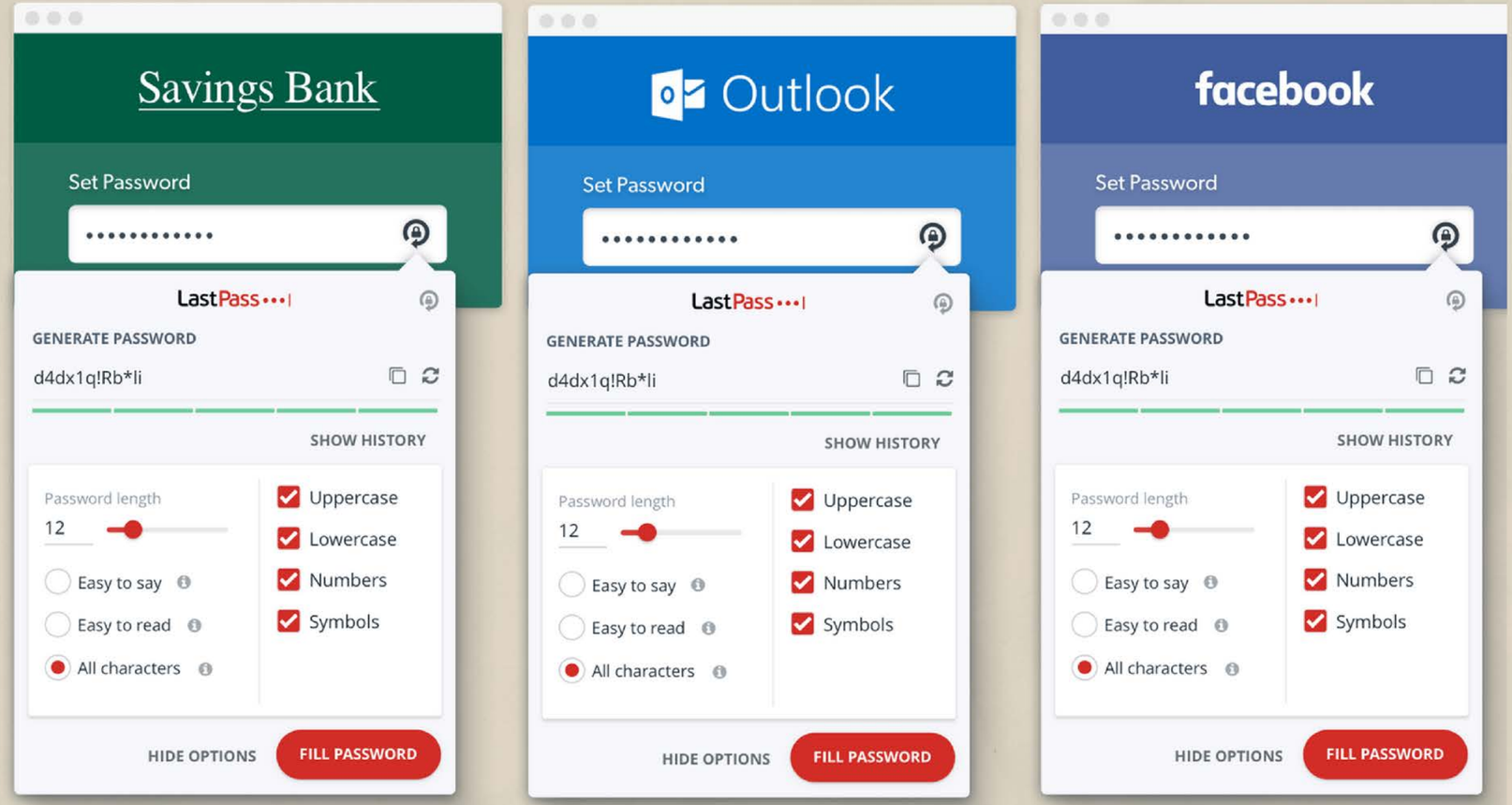
Nachdem Sie ein sicheres Kennwort erstellt haben, sollten Sie dafür sorgen, dass es sicher ist:

Schritt 1. Verstecken Sie geschriebene Passwörter:

Wenn Sie Ihr Passwort aufschreiben müssen, um es sich zu merken, lassen Sie es nicht auf Ihrem Computer oder Schreibtisch liegen. Achten Sie darauf, dass alle aufgeschriebenen Passwörter an einem geheimen oder verschlossenen Ort aufbewahrt werden.

Tip 1 Verwenden Sie ein sicheres Passwort

Schritt II. Verwalten Sie Ihre Passwörter mit einem Tool:



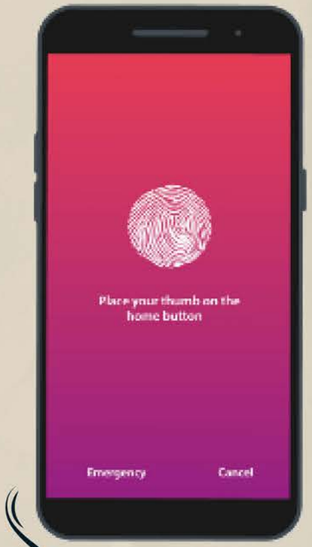
Eine Möglichkeit, Passwörter sicher zu speichern und zu merken, ist die Verwendung eines Tools, das Ihre Liste von Benutzernamen und Passwörtern in verschlüsselter Form speichert. Einige dieser Tools helfen Ihnen sogar, indem sie die Informationen auf bestimmten Websites automatisch für Sie ausfüllen. (Beispiel: LastPass.)

Tip 2

Schützen Sie Ihr Gerät mit einem Passwort

Das Einrichten eines Passcodes auf Ihrem Mobilgerät hilft, unbefugte Benutzer von Ihrem Gerät fernzuhalten, und kann hilfreich sein, wenn Ihr Gerät einmal verloren geht oder gestohlen wird. Jedes Mal, wenn Sie Ihr Gerät einschalten oder aufwecken, werden Sie nach Ihrem Passcode gefragt, bevor Sie das Gerät verwenden können. Im Abschnitt "Sicherheit" Ihres Smart-Geräts werden Ihnen mehrere Sperrtypen zur Auswahl angeboten:

Gesichtserkennungssysteme - Sie können Ihr Gesicht zeigen, um Ihre Identität zu bestätigen. Es wird lediglich eine Person als alleiniger Besitzer des Geräts erkannt, während der Zugang für andere eingeschränkt wird.



Fingerabdruckerkennung - Dies ist eine weitere Form der biometrischen Sicherheit wie die Gesichtserkennung.

PIN - Sie können einen 4-stelligen (bei manchen Geräten 6-stelligen) Code eingeben, um Ihr Gerät zu entsperren

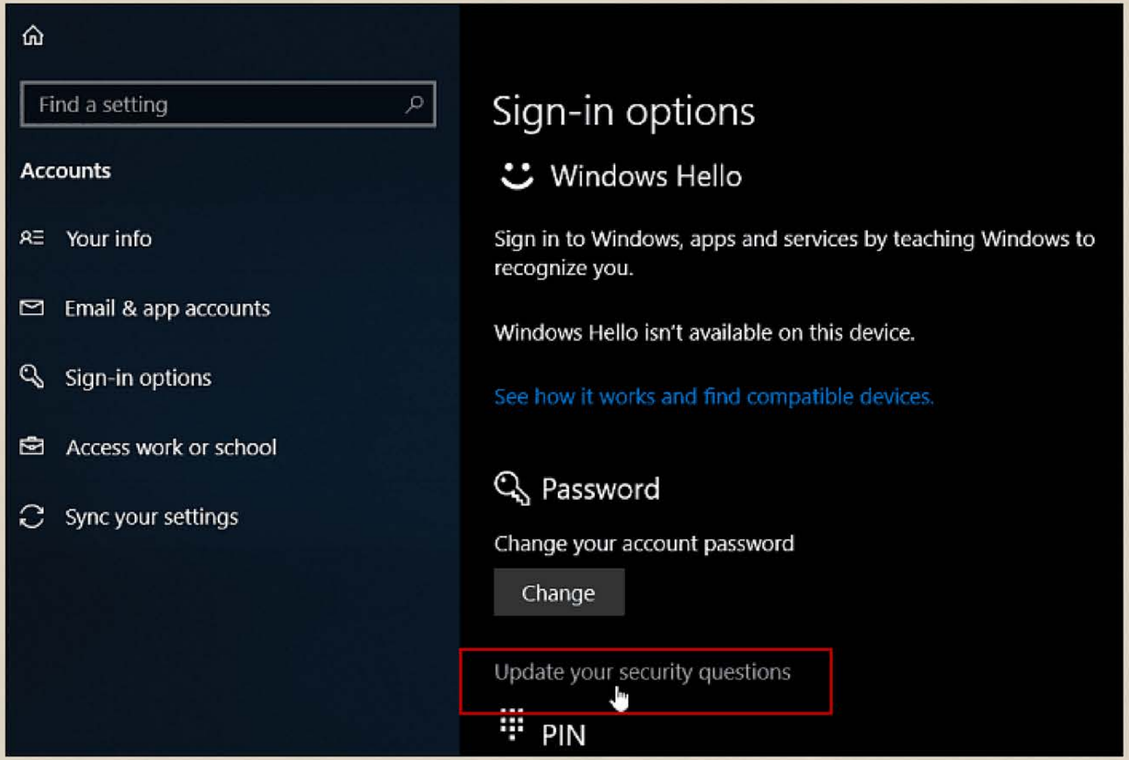
Muster - Sie können ein Muster auf ein Gitter zeichnen, um Ihr Gerät zu entsperren

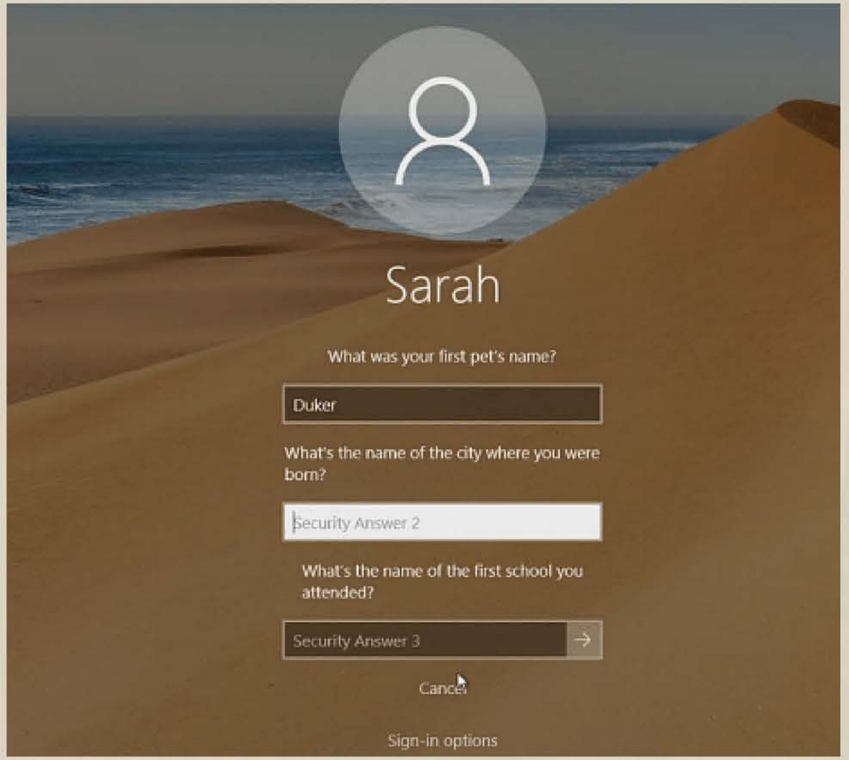
Tip 3 Halten Sie Ihr Gerät auf dem neuesten Stand

Computerentwickler veröffentlichen Updates, um die Sicherheit ihrer Produkte zu gewährleisten. Halten Sie die Software Ihres Geräts auf dem neuesten Stand, damit es nicht anfällig für Malware ist.

Schützen Sie Ihren Computer außerdem durch die Installation von Antiviren-Software.

Tip 4 Richten Sie Ihre Sicherheitsantworten ein





Die Sicherheitsfragen dienen dazu, die Sicherheit Ihres Benutzerkontos zu gewährleisten. Sie werden auch verwendet, um Sie zu identifizieren, wenn Sie Ihr Passwort vergessen haben und nicht auf Ihr Konto zugreifen können. Diese Option ist auf den meisten Websites sozialer Medien verfügbar.

Tip 5

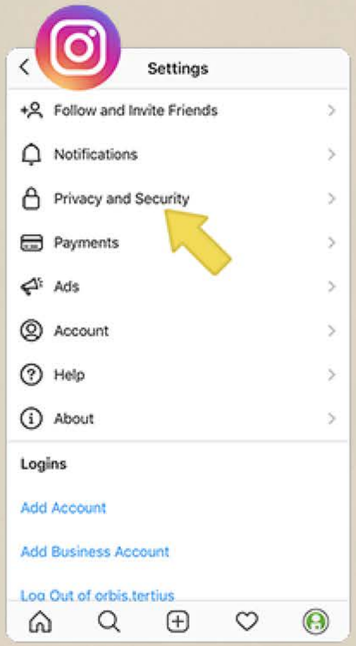
Lernen Sie die Datenschutzeinstellungen kennen

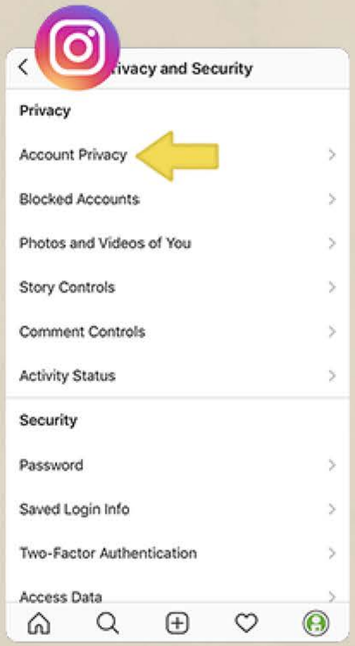
Machen Sie sich mit den Datenschutzrichtlinien für jedes Gerät, jede App und jeden Dienst, den Sie nutzen, vertraut!

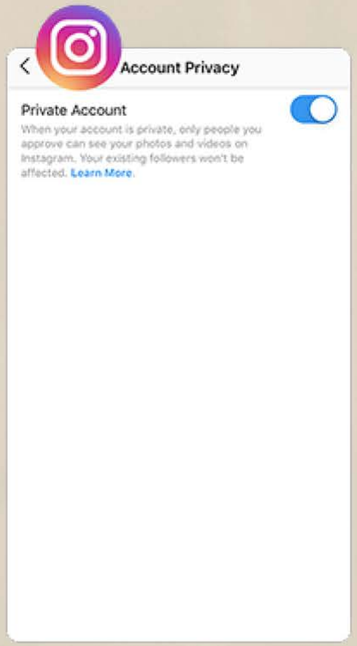
Einige Apps bitten um die Erlaubnis, auf Fotos und andere persönliche Informationen zuzugreifen. Bleiben Sie informiert, damit Sie nichts weitergeben, was Sie nicht wollen.

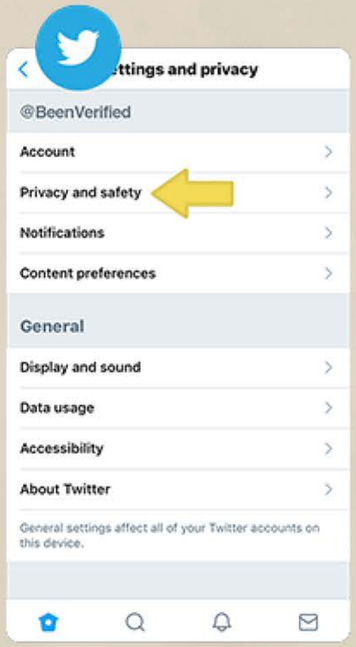
Tip 6

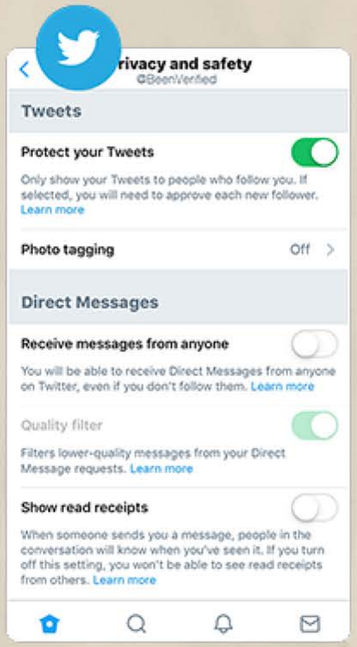
Setzen Sie Ihre Profile auf privat











Überlegen Sie genau, wer Ihre Beiträge und persönlichen Informationen sehen darf. Überlegen Sie, ob Sie Ihre Profile auf "Nur Freunde/Follower" einstellen. Wenn Sie Ihr Profil auf privat setzen, haben nur akzeptierte Follower Zugriff auf die von Ihnen geposteten Inhalte.

Tip 7

Seien Sie vorsichtig mit dem, was Sie teilen

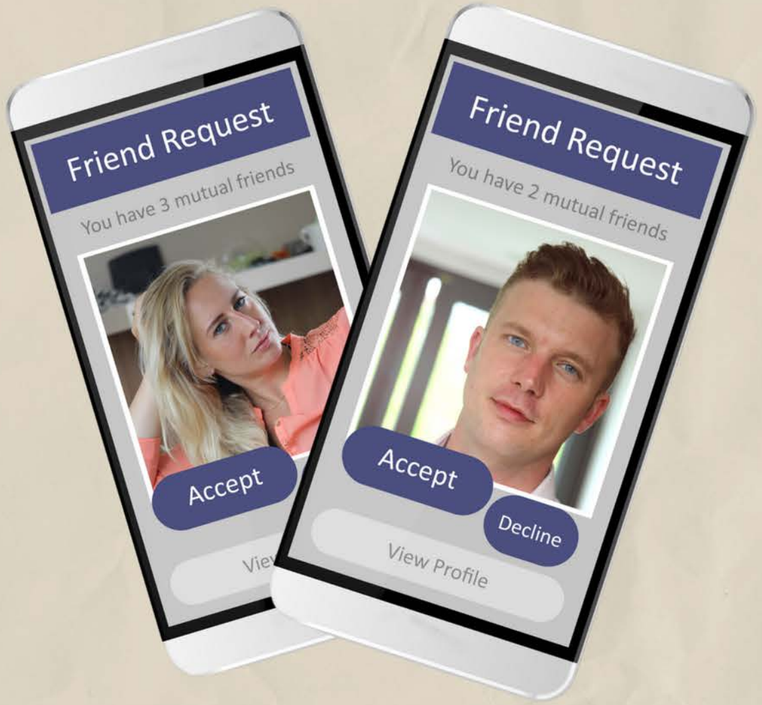
Auch wenn Sie Ihre Privatsphäre gut geschützt haben, müssen Sie sich mit der Tatsache abfinden, dass das, was Sie online veröffentlichen, nie wirklich privat ist und weitergegeben werden kann. Es ist daher wichtig, dass Sie immer erst nachdenken, bevor Sie etwas veröffentlichen.

Tip 8

Seien Sie wählerisch bei freundschaftsanfragen

Wenn Sie die Person nicht kennen, nehmen Sie ihre Anfrage nicht an!

Selbst wenn Sie das tun, klicken Sie auf das Profil, um sicherzugehen, dass es sich nicht um ein gefälschtes Konto handelt, das versucht, auf Ihre vertraulichen Daten zuzugreifen. Cyberkriminelle können sich als Personen ausgeben, die Sie online kennen. Sie können versuchen, Geld zu ergaunern, politische Propaganda zu verbreiten oder andere schändliche Absichten zu verfolgen.



Tip 9

Links mit Bedacht anklicken

Seien Sie vorsichtig bei Websites oder E-Mails mit verdächtigen Links. Einige Websites verwenden Quiz, kostenlose Angebote oder anzügliche Geschichten, um Sie zum Anklicken zu verleiten und dann Ihre persönlichen Daten zu stehlen.

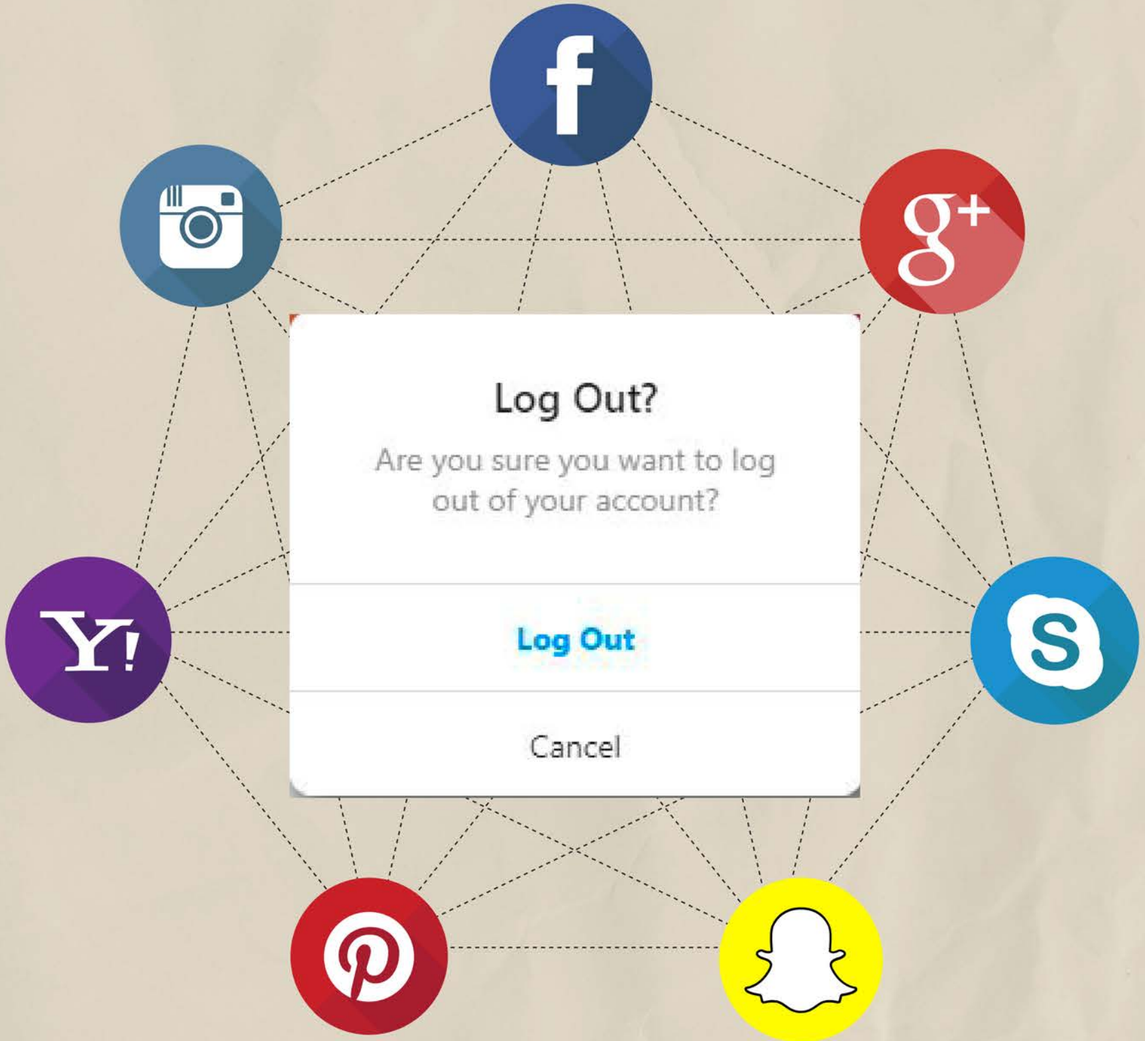
Prüfen Sie die Zuverlässigkeit der Website!

Prüfen Sie dazu, ob die Website ein kleines Schlosssymbol oder "https" vor der URL hat. Das "s" in "https" steht für "sicher" und das Schloss bedeutet, dass die Seite von Ihrem Browser als sicher bestätigt wurde.

Tip 10

Abmelden, wenn Sie fertig sind

Lassen Sie Ihren Browser sich nicht Ihre Anmeldedaten merken. Es ist viel sicherer, wenn Sie Ihre Daten bei jeder Anmeldung neu eingeben, auch wenn das etwas länger dauert.



Datenschutz

&

Digital footprint

"Was lassen Sie zurück?"

Was sind digitale Daten?

Daten: *"Die in einem Computersystem gespeicherten Informationen"*

Auch wenn sich digitale Plattformen als "kostenlos" vermarkten - sie sind es nicht. Social-Media-Unternehmen verdienen an der Datengewinnung - die Nutzer bezahlen für die Dienste mit ihren eigenen Daten und ihrer Privatsphäre.

Das Ziel dieser Unternehmen ist es, jeden dazu zu bringen, so viele Informationen wie möglich über sich selbst zu teilen und so viele Daten wie möglich über jeden zu sammeln. Und sie verwandeln diese Daten in Datenbanken für effiziente, gezielte Werbung.

Welche Daten werden beim Surfen im Internet von Ihnen gesammelt?

Demografische Angaben (z. B. Geburtsdatum, Geschlecht usw.)

Suche Begriffe

Artikel in Ihren Warenkörben und Artikel, die Sie ansehen und kaufen

Browsername (z. B. Chrome, Firefox usw.) und andere Informationen wie die Standardsprache

Die Namen deiner Freunde, wie oft du ein Restaurant besuchst, usw. - überlegen Sie, was Facebook über Sie weiß, wo Sie hingehen und mit wem, usw.

Informationen über Ihr Computersystem, Desktop oder Mobilgerät, CPU- und GPU-Modelle, Bildschirmauflösung usw.

IP Adresse

Standort

Mausbewegungen, Mausklicks und andere Browseraktionen

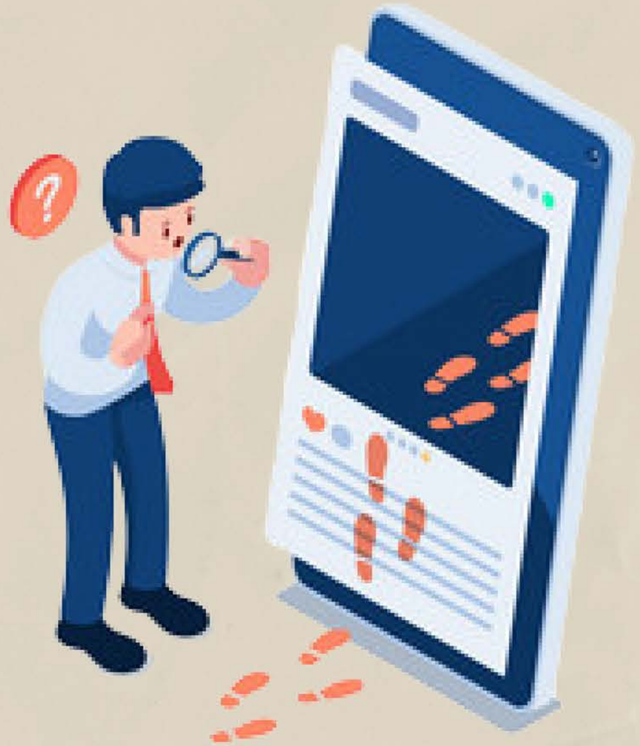
Youtube Videos die Sie gesehen haben

Die Tageszeit, zu der Sie am liebsten im Internet surfen

Webseiten die Sie besucht haben

Wie verwalten Sie Ihren digitalen fußabdruck?

Digitaler Fußabdruck: "Was Sie zurücklassen."



Ein "digitaler Fußabdruck" ist im Grunde Ihre gesamte Online-Präsenz - alle Informationen, Beiträge, Bilder und Daten, die Sie online stellen, ob absichtlich oder unabsichtlich. Je mehr Informationen Sie online stellen, desto mehr können andere über Sie erfahren. Manche Leute können diese Informationen nutzen, um herauszufinden, was Sie kaufen möchten, oder für andere, weniger angenehme Zwecke, wie z. B. den Versuch, sich in unsere Online-Konten zu hacken und an Passwörter, Bankdaten usw. zu gelangen.

Wie verwalten Sie Ihren digitalen fußabdruck?

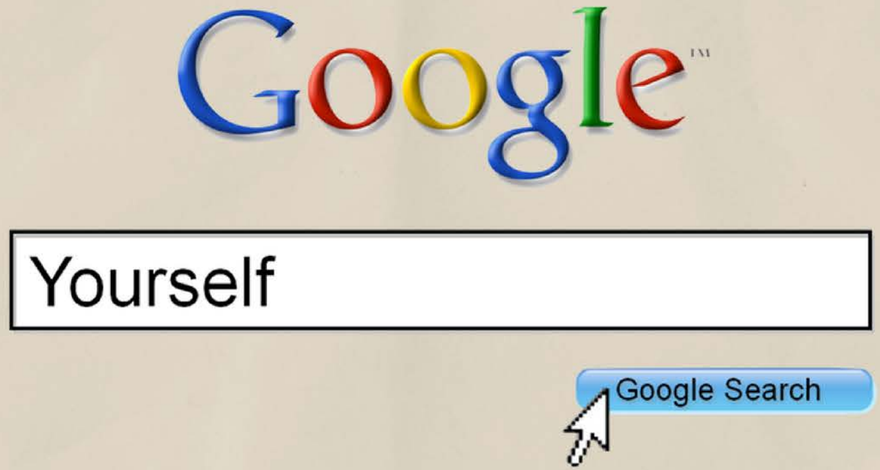
Digitale Fußabdrücke, einschließlich der Metadaten und Inhalte, haben Auswirkungen auf Sicherheit, Privatsphäre und Vertrauen. Da das Internet immer größer wird, wird es immer wichtiger, sich Gedanken darüber zu machen, was mit den Eigentumsrechten an den eigenen Fotos und den von Ihnen geschriebenen Inhalten geschieht. Sie könnten sogar zum Ziel eines digitalen Identitätsdiebstahls werden.

Denken Sie daran, dass das, was ins Internet gestellt wird, in der Regel dort bleibt, auch wenn Sie Beiträge löschen, bleibt eine Spur von Daten zurück.

Hier sind die 10 wichtigsten Maßnahmen, die Sie ergreifen können, um Ihren digitalen fußabdruck zu verringern und zu verwalten

Wie verwalten Sie Ihren digitalen fußabdruck?

1. Suchen Sie selbst im Internet, um zu sehen, was Sie finden.

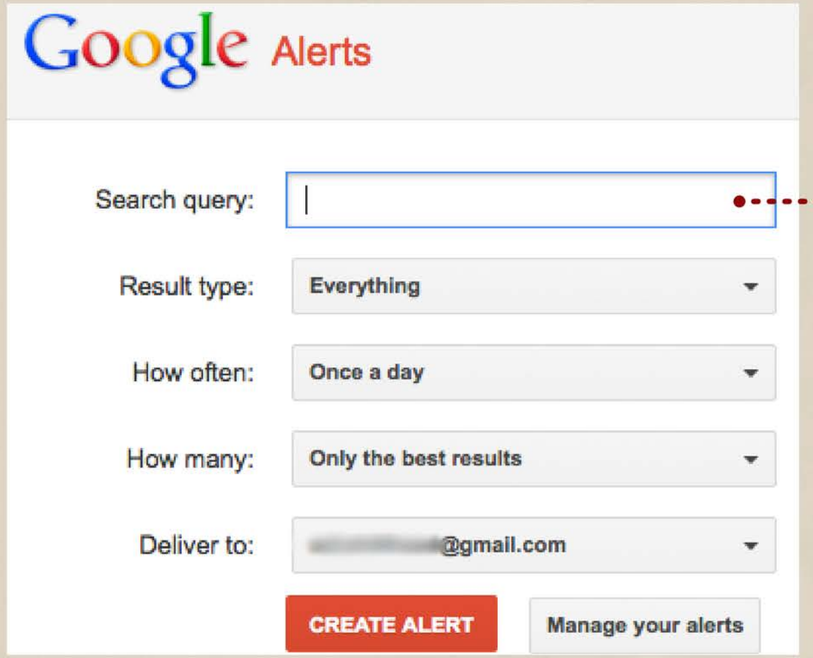


Sie müssen genau wissen, was Ihr digitaler Fußabdruck ist, um ihn gut zu verwalten. Suchen Sie nach sich selbst in verschiedenen Suchmaschinen (Google, Yahoo usw.) und sehen Sie sich die Ergebnisse an, die Sie erhalten. Machen Sie eine Liste mit allem, was Sie gerne loswerden oder verbessern möchten.

Wie verwalten Sie Ihren digitalen fußabdruck?

2. Setzen Sie einen Google-Alarm für Ihren eigenen Namen!

Auf diese Weise erhalten Sie eine Benachrichtigung, wenn etwas über Sie online erscheint.



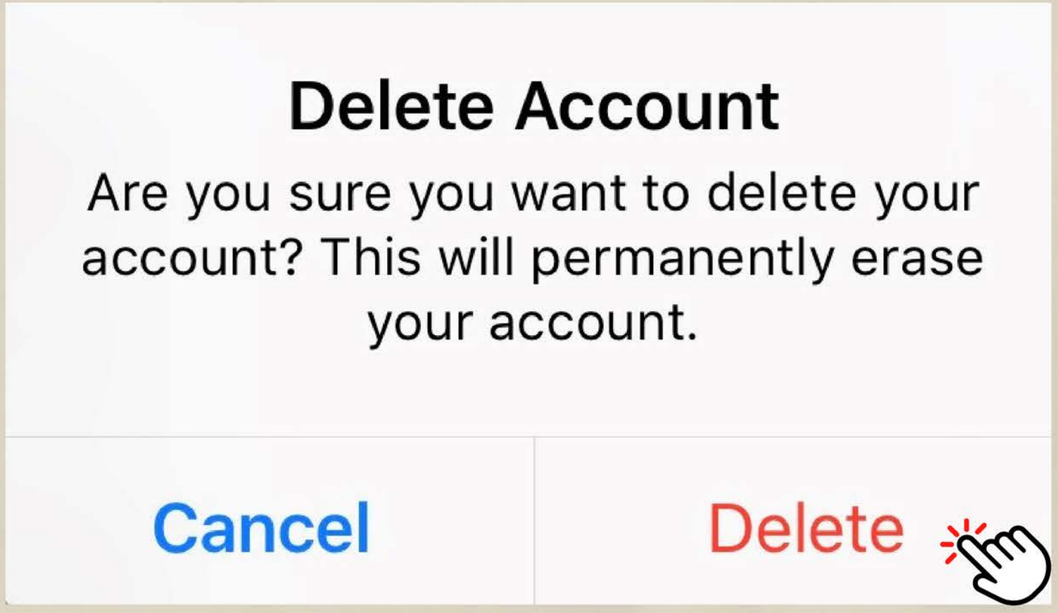
Geben Sie Ihren Name hier ein!

Sie können nicht immer selbst kontrollieren, was online angezeigt wird. Wenn Sie Hilfe benötigen, wenden Sie sich an die Suchmaschine, bei der die Ergebnisse erscheinen, und bitten Sie sie, sie zu löschen. Bei Google zum Beispiel können Sie persönliche oder private Informationen, die in der Suchmaschine auftauchen, auf der Google-Support-Seite melden.

Wie verwalten Sie Ihren digitalen fußabdruck?

3. Schalten Sie Profile oder Konten ab, die Sie nicht mehr verwenden, und stellen Sie Ihre Kontooptionen auf privat.

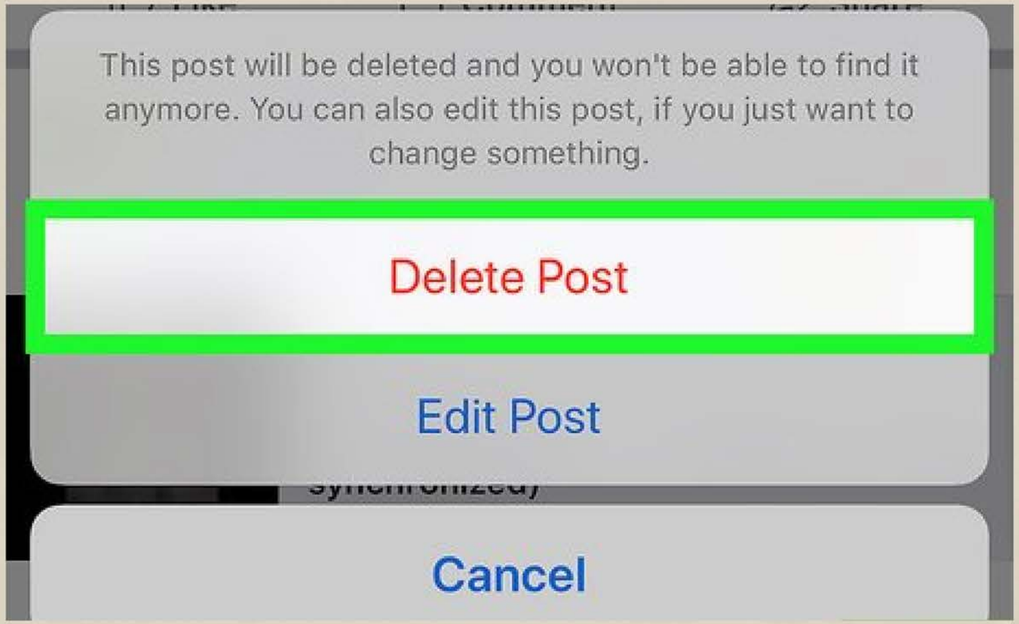
Es macht keinen Sinn, Konten zu führen, die Sie nicht nutzen. Wenn Sie all diese Konten geöffnet haben, erhöht sich nur die Menge der Informationen über Sie im Internet. Das macht Ihre Online-Präsenz unübersichtlich. Schließen oder löschen Sie daher alle Konten, die Sie nicht mehr nutzen.



Außerdem sollten Sie auf allen anderen Plattformen die Einstellungen auf "privat" setzen, um zu kontrollieren und einzuschränken, wer Ihre Beiträge sehen kann.

Wie verwalten Sie Ihren digitalen fußabdruck?

4. Löschen Sie alles, was Sie nicht gut repräsentiert.



Wenn Sie nach sich selbst suchen, finden Sie möglicherweise einige unprofessionelle Beiträge. Das bedeutet, dass jeder sie sehen kann, was Ihnen in Ihrem Privat- und Berufsleben schaden könnte. Zu den fragwürdigen Inhalten gehören in der Regel Obszönitäten, pikante Fotos, Alkoholkonsum oder unhöfliche Kommentare. Löschen Sie diese, wenn sie auftauchen, und verzichten Sie in Zukunft auf weitere Einträge.

Wie verwalten Sie Ihren digitalen fußabdruck?

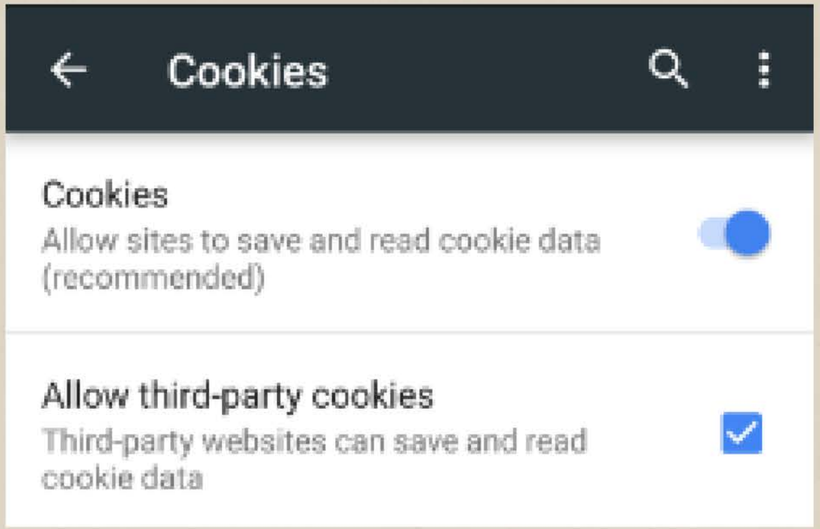
5. Denken Sie nach, bevor Sie posten.

Denken Sie über alle Auswirkungen Ihrer Beiträge nach und teilen Sie nur Dinge, die Sie in einem positiven, professionellen Licht zeigen. Versuchen Sie zu vermeiden, etwas zu posten, wenn Sie emotional oder wütend sind. Sie denken dann vielleicht nicht über die größeren Auswirkungen Ihrer Äußerungen nach.

Denken Sie daran, dass die Verwendung von Privatsphäre-Einstellungen kein Ersatz dafür ist, vorsichtig zu sein, was Sie posten. Vermeiden Sie dennoch unangemessene Beiträge, auch wenn Ihre Konten gesperrt sind.

Wie verwalten Sie Ihren digitalen fußabdruck?

6. Löschen Sie Cookies alle paar Monate, um Tracking-Daten zu löschen.



Cookies werden verwendet, um Ihre Suchdaten für bestimmte Websites zu verfolgen. Dies soll Ihr Web-Erlebnis bequemer machen, weil sich die Websites an Sie erinnern, aber es könnte auch Ihre persönlichen Informationen speichern.

Um dies zu vermeiden, sollten Sie es sich zur Gewohnheit machen, die Cookies Ihres Webbrowsers alle paar Monate zu löschen, um alles loszuwerden, was Ihre Aktivitäten verfolgen könnte.

Wie verwalten Sie Ihren digitalen fußabdruck?

7. Achten Sie auf verdächtige Nachrichten und Phishing-E-Mails.

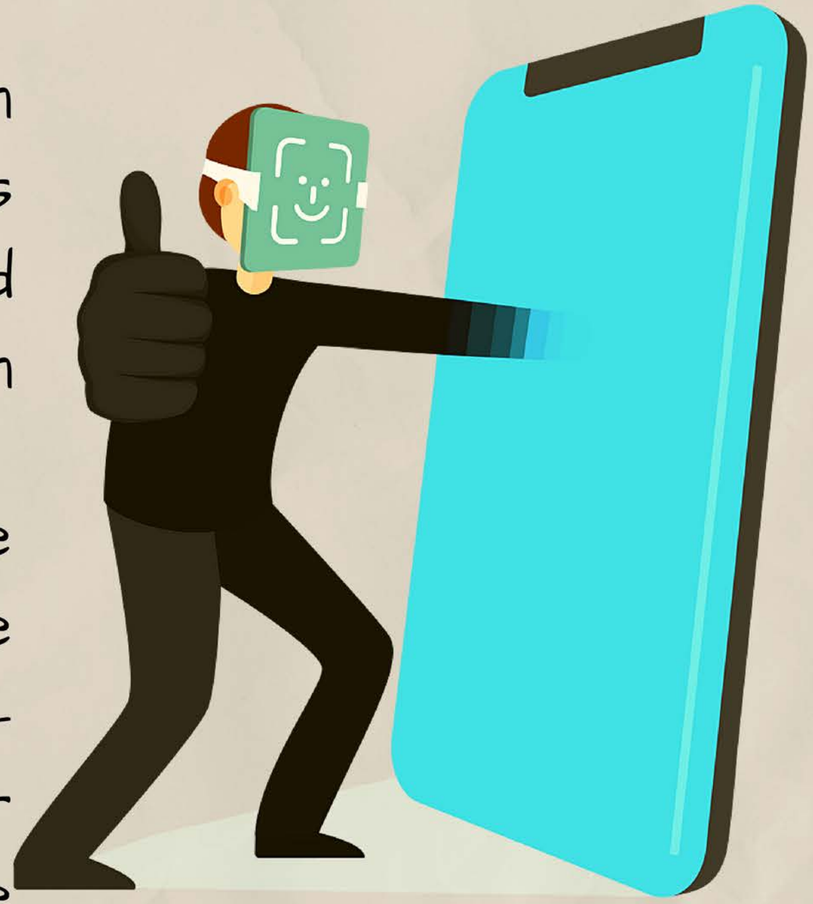
Nachrichten mit einer verkürzten URL zusammen mit einer Aussage wie "OMG, sieh dir dieses Bild von dir an..." oder "Hast du gesehen, was sie über dich sagen..." ist nicht zu trauen. Klicken Sie nicht auf Links, die in solchen Texten enthalten sind.

Auch Phishing-E-Mails sind ein Problem. Dabei handelt es sich um gefälschte Mitteilungen, die vorgeben, eine vertrauenswürdige Organisation wie Facebook zu sein, und die versuchen, Sie dazu zu bringen, sich anzumelden und Ihre Daten zu stehlen.

Wie verwalten Sie Ihren digitalen fußabdruck?

8. Erkennen Sie die Fälschungen.

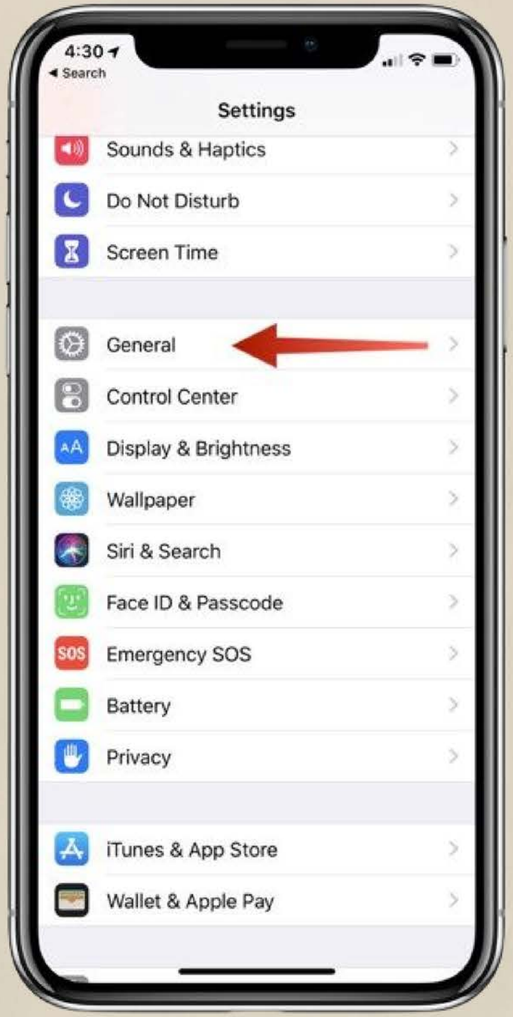
Nicht jeder, der sich in den sozialen Medien bewegt, ist der, für den er sich ausgibt. Es kann Leute geben, die vorgeben, jemand anderes zu sein und Ihnen Schaden zufügen könnten. Sie können zum Beispiel Sie wollen Sie dazu bringen, private oder persönliche Informationen preiszugeben, die sie gegen Sie verwenden könnten. Wenn Sie einmal einen Online-Freund gefunden haben, muss das nicht von Dauer sein. Überprüfen und bereinigen Sie Ihre Kontakte regelmäßig.

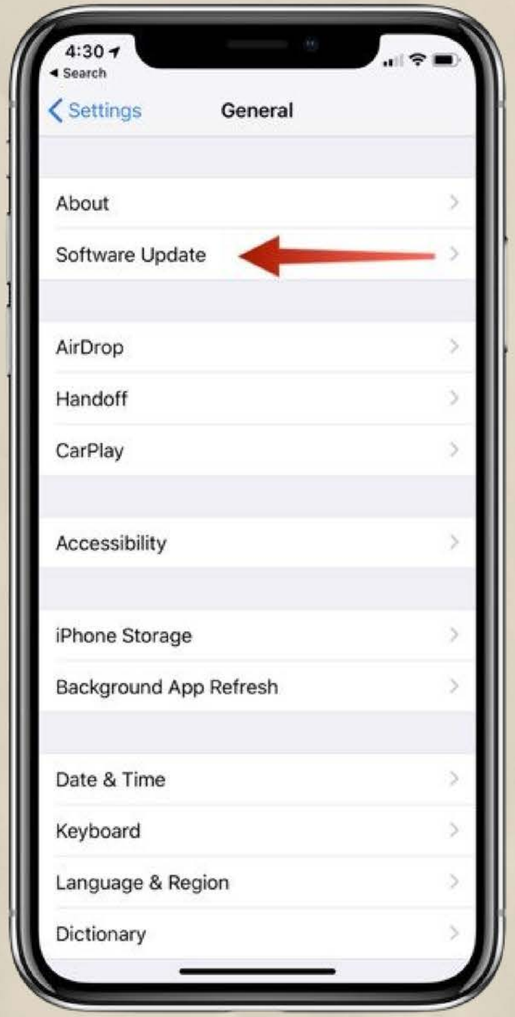


Wie verwalten Sie Ihren digitalen fußabdruck?

9. Aktualisieren Sie immer Ihre Software.

Veraltete Software kann Hackern eine Hintertür für den Zugriff auf Ihre privaten Daten bieten. Wenn Sie Ihr Antivirenprogramm und andere Programme auf dem neuesten Stand halten, erhalten Sie Sicherheits-Patches, mit denen Fehler in Ihrem System behoben oder entfernt werden. Sie können Programme und Anwendungen so einstellen, dass sie automatisch aktualisiert werden, damit Sie sicher sein können, dass Sie die neueste Software installiert haben.

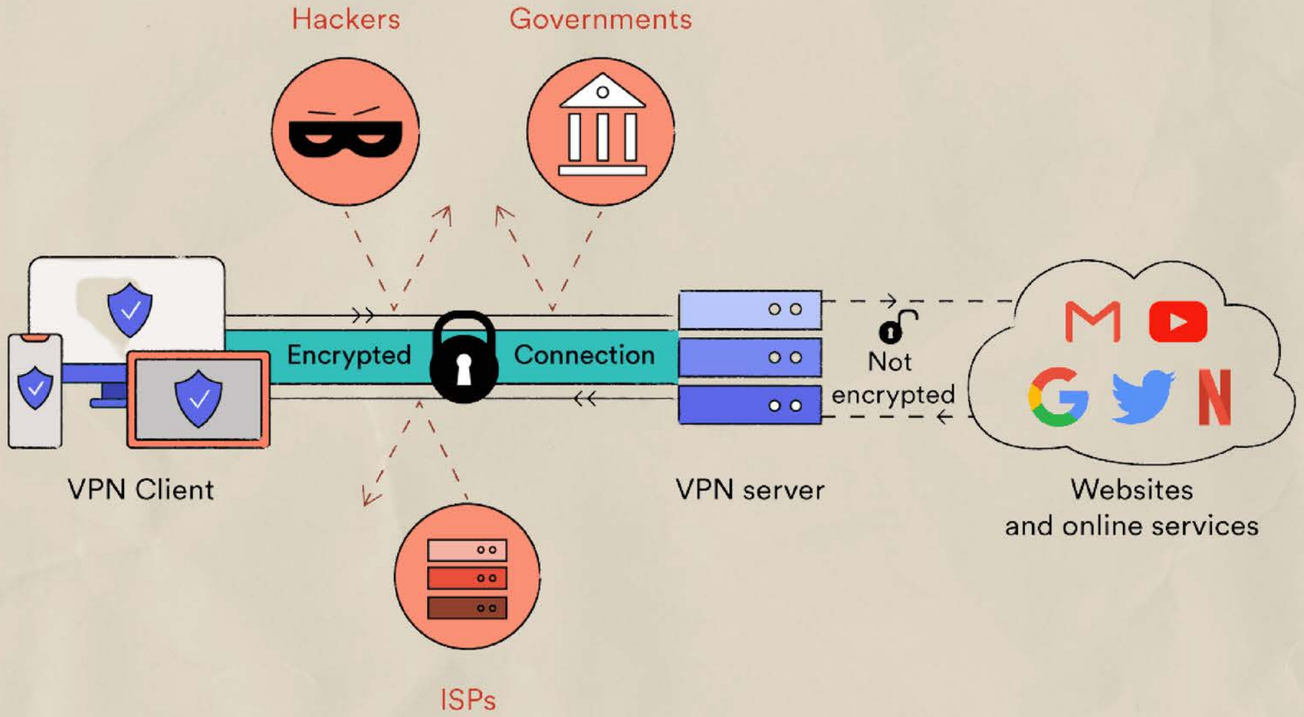




Wie verwalten Sie Ihren digitalen fußabdruck?

10. Verwendung von Tools für virtuelle private Netzwerke.

Um Ihre Privatsphäre zu schützen, können Sie Anti-Tracking-Tools, private Suchmaschinen oder anonyme Browser verwenden. Virtuelle private Netzwerke (VPNs) maskieren Ihre IP-Adresse, damit Sie Ihren Standort, Ihren Browserverlauf und andere Informationen geheim halten können.



New Tab

Cyber-Mobbing und einfache Hassreden

Was bedeutet Cyber-Mobbing?

Wie schützen Sie sich?

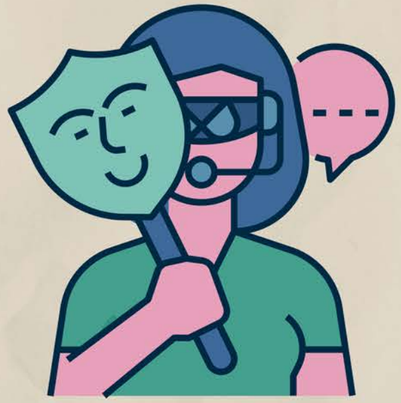
Wie kann ich andere schützen?

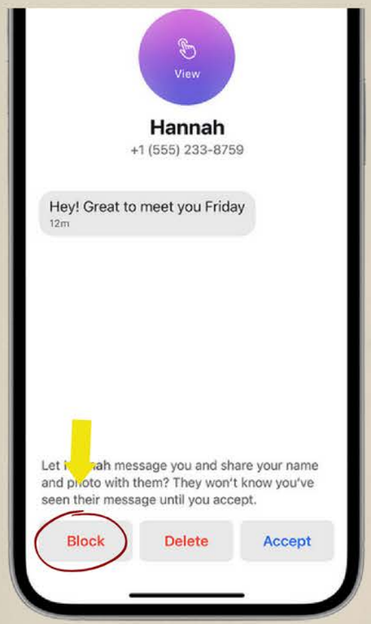
Was bedeutet Cyber-Mobbing?

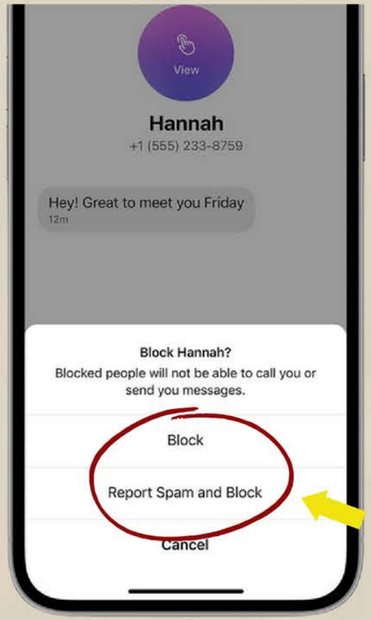
Es gibt viele soziale Plattformen, auf denen Menschen verschiedene Inhalte erstellen und teilen. Eine der größten Gefahren dabei ist, dass die Nutzer aufgrund des Bedürfnisses nach Verbindung, Aufmerksamkeit und Anerkennung oft rücksichtslos handeln. Was sie im wirklichen Leben nicht tun würden, können sie im Internet viel leichter und mit weniger Hemmungen tun. Dieser Missbrauch von Informationstechnologien mit der Absicht, anderen zu schaden, wird als Cyber-Mobbing bezeichnet.

Wie lässt sich Cybermobbing verhindern?

Virtuelle Nutzer missbrauchen soziale Plattformen, um ihre so genannten "Freunde" zu belästigen. Manchmal verwenden diese Personen gefälschte Identitäten und Konten oder greifen auf Anonymisierungswerkzeuge zurück, um ihre Identität zu verbergen, damit sie andere hinter virtuellen Masken schikanieren können.







Es gibt 7 einfache Schritte, um Cyber-Mobbing zu verhindern:

- Verbessern Sie Ihre Privatsphäre.
- Wählen Sie, nicht zu antworten.
- Blockieren Sie die Person oder Personen.
- Nicht zu viel teilen.
- Sprechen Sie mit jemandem.
- Sichern Sie die Beweise.
- Meldung an Plattformen/Behörden.

Seien Sie sich der Auswirkungen Ihrer Beiträge auf andere bewusst

Manchmal denken die Leute, dass das, was sie tun, harmlos oder nur ein Scherz ist, wenn sie ein Video oder ein Bild veröffentlichen, das jemanden in Verlegenheit bringt, oder Ratschläge über alternative Medizin aus nicht vertrauenswürdigen Quellen weitergeben, usw.

Aber die Wahrheit ist, dass die digitale Welt eine reale Welt mit realen Konsequenzen ist. Sobald Sie etwas posten, verlieren Sie die Kontrolle über die sozialen, traumatischen und psychologischen Auswirkungen auf eine Person, die Sie teilen.

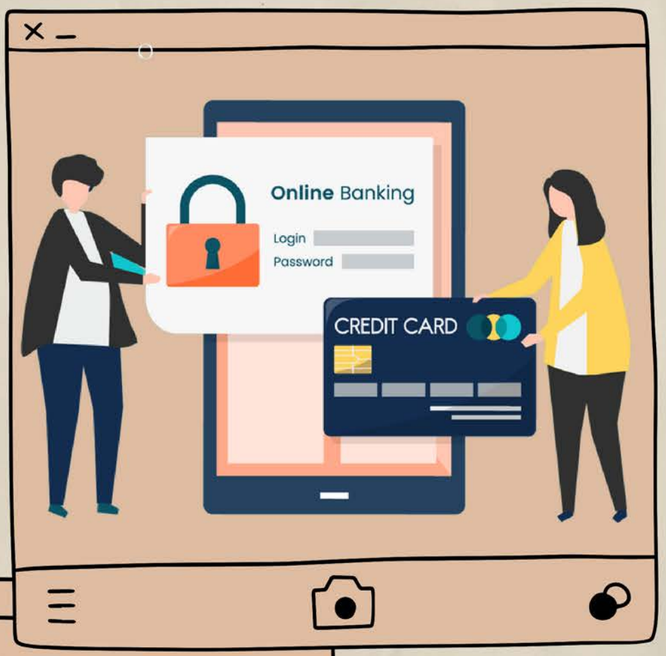
Missbrauchen Sie soziale Netzwerke nicht, um andere zu beschämen und zu schikanieren!

fragen Sie sich immer folgendes, bevor Sie auf Senden klicken!

Erwägen Sie diese 10 Fragen bevor Sie Entsendung.

1. Werde ich mich später gut oder anders fühlen?
2. Warum poste ich?
3. Würde ich das persönlich sagen?
4. Kann man das anders interpretieren?
5. Bin ich freundlich?
6. Würde ich mich mögen?
7. Ist es wirklich privat?
8. Habe ich die Erlaubnis?
9. Ist das legal?
10. Ist es genau?

Online Einkauf & Banking



Was ist Onlinebanking?

Online und Mobile Banking ist eine sichere Möglichkeit, Ihre Finanzen bequem von zu Hause oder von unterwegs aus zu verwalten.

Wofür kann ich Onlinebanking nutzen

- Prüfen Sie Ihr Guthaben.
- Prüfen Sie Ihre Bank Auszüge.
- Überweisen Sie Geld zwischen Ihren Bankkonten
- Rechnungen bezahlen
- Geld an Menschen schicken.
- Einrichten oder Stornieren von Lastschriften Abbuchungen und Daueraufträge.

Wie richte ich Onlinebanking ein?

Solange Sie über ein Gerät mit Internetzugang und ein Konto bei einer Bank verfügen, die für Online-Banking zugelassen ist, können Sie ganz einfach loslegen:

Um Zugang zum Online-Banking zu erhalten, müssen Sie sich zunächst auf der Website Ihrer Bank registrieren. Jede Bank hat ein etwas anderes Verfahren für die Einrichtung des Online-Bankings, und Sie sollten mit Ihrer Bank sprechen.

Die folgenden Schritte sind möglich:

·Eingabe Ihrer persönlichen Daten und Ihrer Bankverbindung (Bankleitzahl und Kontonummer).

- Die Bank kann Sie anrufen und Ihnen einige Fragen stellen, um Ihre Identität zu überprüfen, und Ihnen einen Aktivierungscode oder eine SMS schicken.

- Einrichtung eines Benutzernamens und eines sicheren Passworts oder Passcodes.

Was kann ich tun, um mein Geld und meine Identität zu schützen?

1. Verwenden Sie für den Zugriff auf Ihr Online-Banking nur sichere WLAN-Netze und -Geräte.

Wenn Sie öffentliche Netze nutzen, z. B. in Cafés oder Bahnhöfen, kann es möglich sein, dass Personen, die sich im selben Netz befinden, auf Ihre Daten zugreifen. Seien Sie auch vorsichtig, wenn Sie einen öffentlichen Computer für den Zugriff auf Ihr Online-Banking verwenden. Diese verfügen möglicherweise nicht über die richtige Sicherheitssoftware.

Was kann ich tun, um mein Geld und meine Identität zu schützen?

2. Verwenden Sie unterschiedliche Anmeldedaten und Passwörter für Online-Bankkonten.

Verwenden Sie keine der Anmeldedaten, die Sie für das Online-Banking verwenden, für andere Online-Portale oder -Dienste. Achten Sie darauf, ein sicheres Passwort zu erstellen und es regelmäßig zu ändern.

3. Geben Sie Ihre Anmeldedaten für das Online-Banking an niemanden weiter.

Behalten Sie sie für sich, ebenso wie Pin-Codes und andere sensible Authentifizierungsdaten.

Was kann ich tun, um mein Geld und meine Identität zu schützen?

4. Achten Sie darauf, an wen Sie Geld überweisen.

Überweisen Sie Geld nur an Personen, denen Sie vertrauen. Eine Geldüberweisung kann in der Regel nicht ohne die ausdrückliche Zustimmung des Empfängers rückgängig gemacht werden.

Was kann ich tun, um mein Geld und meine Identität zu schützen?

5. Verwenden Sie Software zum Schutz vor Identitätsdiebstahl oder ein VPN.

Erwägen Sie das Herunterladen einer Software zum Schutz vor Identitätsdiebstahl. Dabei handelt es sich um einen Dienst, der Ihre Internetverbindung verschlüsselt, um sie sicher zu halten. Diese Dienste bieten oft mehrere Schutzmaßnahmen in einem Paket an, darunter ein VPN und eine Passwortüberwachung.

Sicher online einkaufen

Der Online-Einkauf kann das Leben sehr viel einfacher machen und den Gang zum Supermarkt oder Einkaufszentrum überflüssig machen. Sie können in den meisten Supermärkten, in großen Geschäften und auch in kleineren unabhängigen Geschäften online einkaufen.

Die Waren können direkt zu Ihnen nach Hause geliefert werden, in der Regel gegen eine geringe Gebühr oder kostenlos, oder Sie können auch einen Service namens "Click and Collect" in Anspruch nehmen, bei dem Sie online bestellen und die Artikel im Geschäft abholen.

Aber es ist wichtig, sichere und seriöse Websites zu nutzen. Hier sind einige Tipps zum Schutz Ihres Geldes und Ihrer persönlichen Daten beim Online-Einkauf.

Sicher online einkaufen

Tipp 1: Wählen Sie die Website, auf der Sie einkaufen, sorgfältig aus und kaufen Sie bei seriösen Händlern ein.

Wählen Sie Online-Händler mit einem guten Ruf, z. B. bekannte Supermärkte, Geschäfte in der Innenstadt oder etablierte Online-Shops. Achten Sie auf die vollständigen Kontaktinformationen des Unternehmens. Ein seriöses Unternehmen wird diese Informationen immer auf seiner Website angeben. Suchen Sie im Internet nach dem Namen des Unternehmens, um herauszufinden, ob jemand bereits Probleme mit dem Händler hatte.

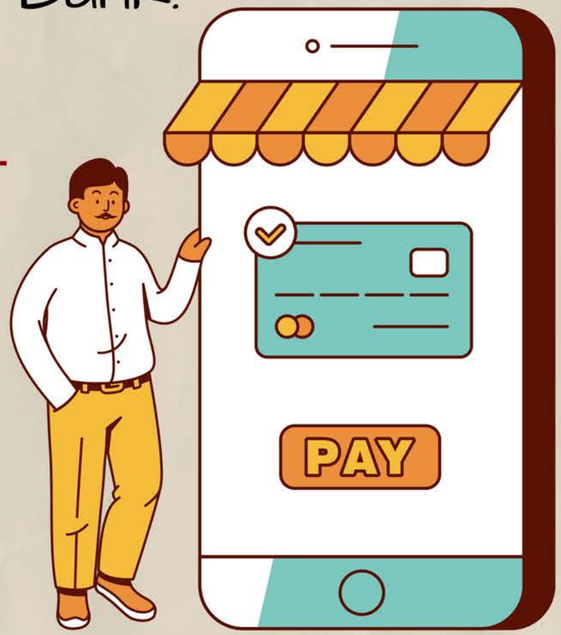
Shopping safely online

Tipp 2: Verwenden Sie dieselbe Karte nur für Internettransaktionen.

Prüfen Sie den Kontoauszug dieser Karte regelmäßig auf ungewöhnliche Transaktionen und wenden Sie sich im Falle eines Problems sofort an Ihre Bank.

Tipp 3: Verwenden Sie für Transaktionen im Internet eine Kreditkarte und keine Debitkarte.

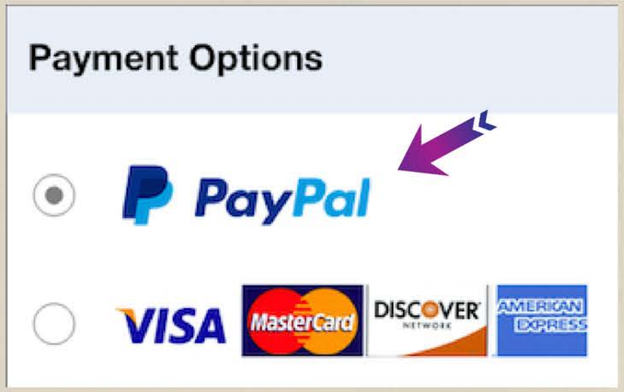
Bietet er zusätzlichen Schutz. Wenn Ihr Kauf mehr als 100 GBP kostet und Sie eine Kreditkarte verwenden, sind der Verkäufer und Ihr Kartenunternehmen gleichermaßen verantwortlich, wenn etwas schiefgeht.



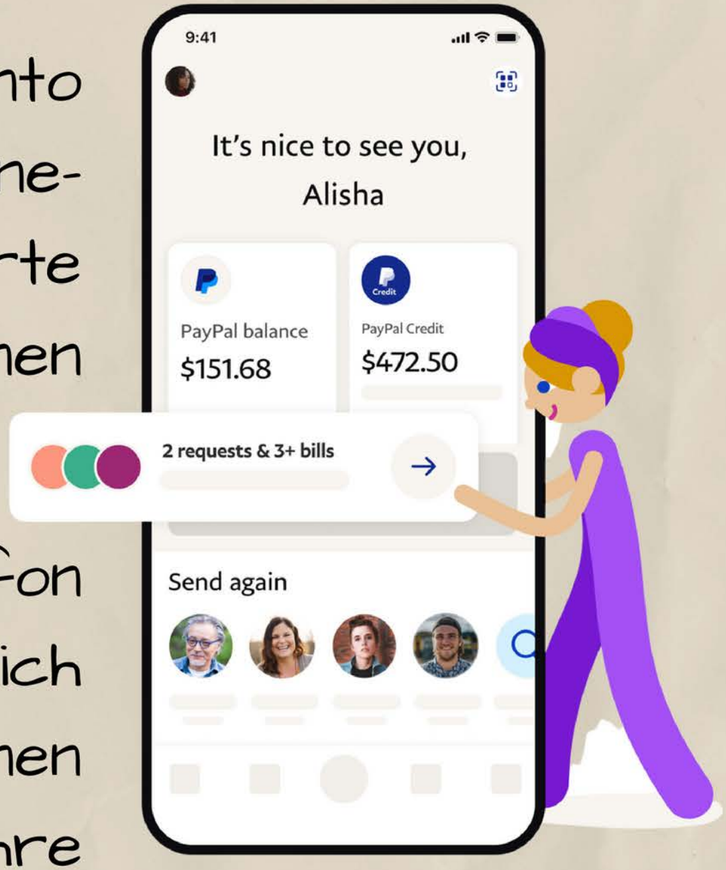
Sicher online einkaufen

Tipp 4. Erwägen Sie die Verwendung eines PayPal Kontos.

Dies ist ein Online-Konto, das Sie mit Ihrem Bankkonto oder Ihrer Zahlungskarte verknüpfen, um Online-Einkäufe zu bezahlen. Wenn Sie keine Kreditkarte verwenden möchten, ist PayPal sicher und bietet einen besseren Zahlungsschutz als eine Debitkarte.



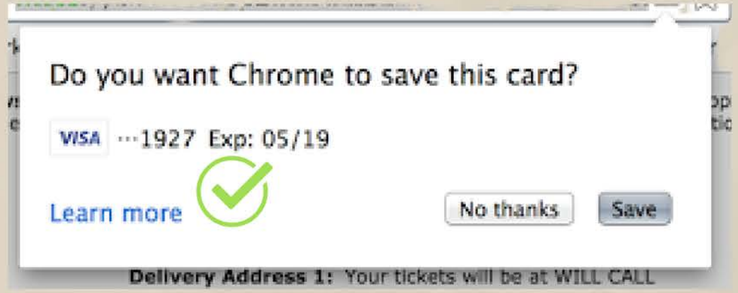
Laden Sie die App auf Ihr Telefon herunter oder melden Sie sich kostenlos online an. Danach können Sie sie als Zahlungsoption für Ihre Einkäufe nutzen.

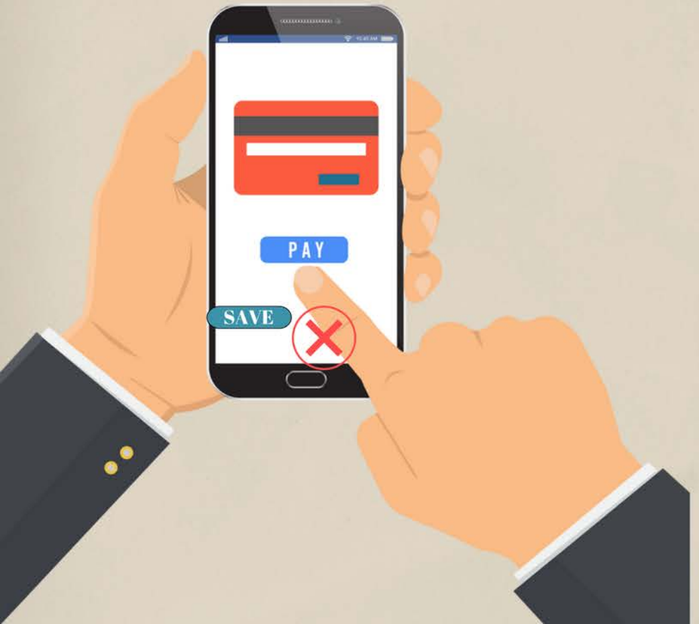


Sicher einkaufen im Internet

Tipp 5. Speichern Sie Ihre Kartendaten nicht.

Manchmal fordert die Website oder Ihr Internet-Browser Sie auf, Ihre Kartendaten für das nächste Mal zu speichern.





Tun Sie dies niemals auf einem gemeinsam genutzten Computer, und stellen Sie sicher, dass Ihr Gerät mit einem Passwort, einer PIN oder einem Fingerabdruck geschützt ist, wenn Sie Ihre Kartendaten speichern.

Sicher online einkaufen

6. Fallen Sie nicht auf E-Mail-Betrug herein

Sie könnten E-Mails oder SMS erhalten, in denen Ihnen tolle Schnäppchen angeboten werden oder in denen behauptet wird, dass es ein Problem bei der Zustellung eines Pakets gegeben hat. Löschen Sie verdächtige Nachrichten von unbekannten Absendern. Und öffnen Sie keine Anhänge oder klicken Sie nicht auf Links in Nachrichten, da diese Ihren Computer oder Ihr Telefon mit Viren und anderer Malware infizieren könnten.

Sicher online einkaufen

7. Verfolgen Sie Ihre Lieferung.

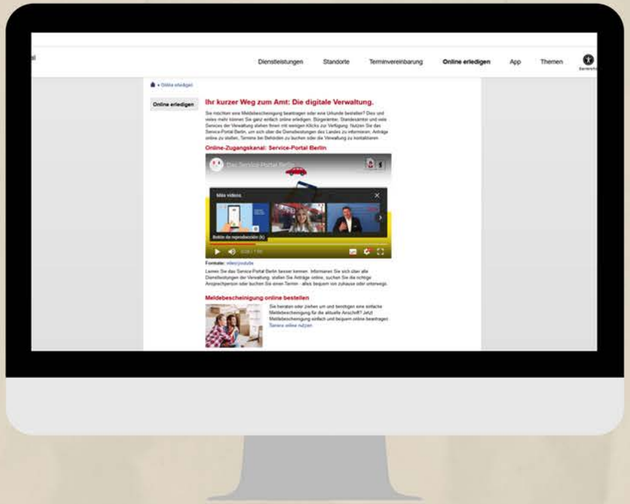
Nachdem Sie einen Online-Kauf getätigt haben, sollten Sie die Bestellung im Auge behalten, um sicherzugehen, dass sie auf dem Weg zu Ihnen ist. Wenn der Händler sich weigert, Versandinformationen anzugeben oder auf Ihre Anfragen zum Status Ihrer Bestellung zu reagieren, wenden Sie sich an Ihren Kreditkartenaussteller. Er kann die Belastung von Ihrer Rechnung entfernen und die Angelegenheit prüfen.

ONLINE ZUGANG ZU ÖFFENTLICHEN DIENSTLEISTSUNGEN

Was sind die elektronischen öffentlichen Dienste in Deutschland?

Service-Portal Berlin - die digitale Verwaltung

In Deutschland gibt es einen föderalen Staat. Es gibt den Staat (Bund), die Länder und die Gemeinden, also die Städte und Gemeinden. Die meisten Dienstleistungen für die Bürgerinnen und Bürger werden von der kommunalen Verwaltung erbracht. Wie das funktioniert, wollen wir am Beispiel von Berlin zeigen.



Berlin hat eine eigene Verwaltung, Bürgerämter und Dienstleistungen. Bürgerbüros, Standesämter und viele Dienstleistungen der Verwaltung sind mit wenigen Klicks für Sie erreichbar.

Service-Portal Berlin - die digitale Verwaltung

Über das Berliner Serviceportal können Sie sich über die Leistungen des Landes informieren, Anträge online stellen,Termine bei Behörden buchen oder Kontakt mit der Verwaltung aufnehmen.

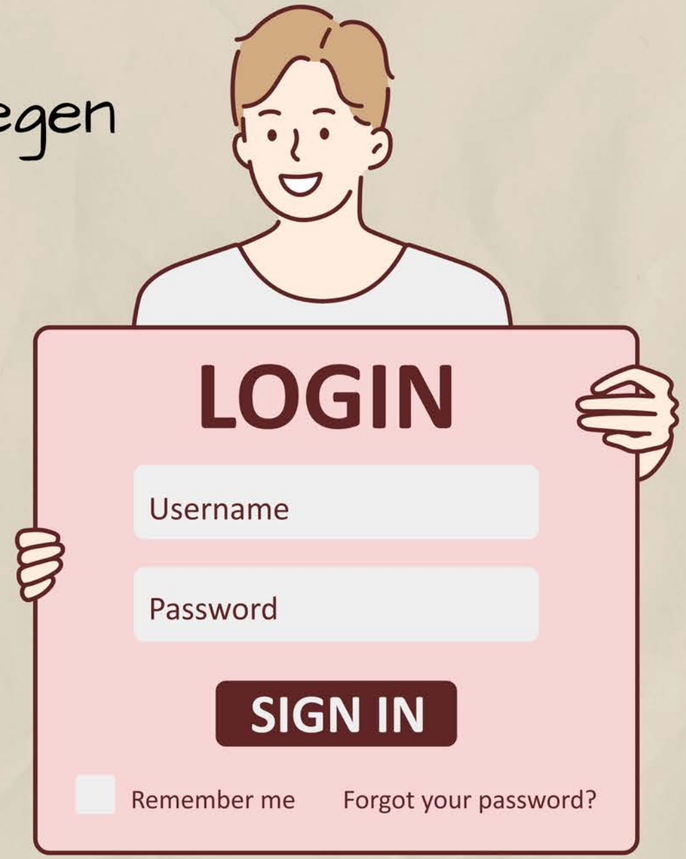
Hier können Sie sich über alle Dienstleistungen der Verwaltung informieren. Es gibt auch eine App, die Sie auf Ihrem Handy nutzen können.

https://service.berlin.de/online-erledigen/

Service-Portal Berlin - die digitale Verwaltung

Sie können

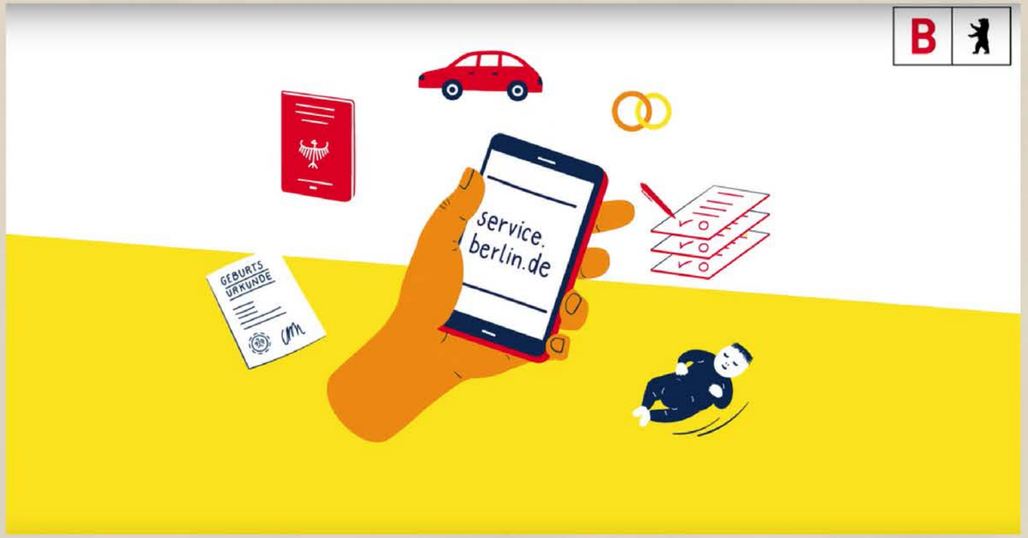
- Anträge online stellen
- Termine im Bürgerbüro vereinbaren
- zuständige Stelle und Ansprechpartner für Ihr Anliegen finden
- eine Wohnung anzumelden
- einen neuen Personalausweis zu beantragen
- Ihr Auto anzumelden
- ein Gewerbe anzumelden.
- uzw.



Service-Portal Berlin - die digitale Verwaltung

Sie können verfügbare Termine in ganz Berlin einsehen und diese buchen, stornieren oder ändern.

Viele Dienstleistungen der Verwaltungen werden in andere Sprachen übersetzt und erklärt. Zum Beispiel Türkisch, Arabisch, Ukrainisch, Polnisch und Englisch.



Es gibt auch einen Chatbot, den Sie zu jeder Tages- und Nachtzeit kontaktieren können und der versuchen wird, Ihnen bei Ihren Fragen auf automatisierte Weise zu helfen. Der Chatbot ist ebenfalls in verschiedenen Sprachen verfügbar.

REFERENCES

BLEIBEN SIE SICHER IN DEN SOZIALEN MEDIEN

https://safety.google/security/security-tips/

https://us.norton.com/internetsecurity-privacy-password-security.html

https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/staying-safe-on-social-media/

https://www.facebook.com/help/122006714548814

DATENSCHUTZ & DIGITAL FOOTPRINT

https://www.gov.uk/data-protection

https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints

https://www.security.org/digital-safety/

https://staysafeonline.org/online-safety-privacy-basics/5-ways-spot-phishing-emails/

REFERENCES

CYBER-MOBBING

https://www.researchgate.net/publication/358402280_Bullying_Cyberbullying_and_Hate_Speech

https://www.unicef.org/end-violence/how-to-stop-cyberbullying

https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/think-before-you-post/

https://www.brandwatch.com/reports/cyberbullying-2016/

ONLINE BANKING & EINKAUFEN

https://www.ageuk.org.uk/globalassets/age-uk/documents/digital-instruction-guides/a-beginners-guide-to-staying-safe-online.pdf

https://www.consumerfinance.gov/about-us/blog/online-mobile-banking-tips-beginners/

https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/

REFERENCES

ONLINE ZUGANG ZU ÖFFENTLICHEN DIENSTLEISTUNGEN

https://service.berlin.de/online-erledigen/

SCAN ME

SCAN ME

Projekt "DIGITALIZE – tools for Roma adults to use the internet and promote education"

Amaro Foro e.V.
facebook.com/AmaroForo/
instagram.com/amaro_foro/

EGYÜTT HATÓ
KÖZÖSSÉGÉPÍTŐ EGYESÜLET
facebook.com/EgyuttHato/
instagram.com/egyutthato/

NEVO PARUDIMOS
facebook.com/NevoParudimos/
instagram.com/nevoparudimos/

RROMA
facebook.com/rromassn.org/
instagram.com/rromassn/

SCAN ME

SCAN ME

SCAN ME