Checkliste

Wie man seine Daten online schützt

kaspersky BRING ON THE FUTURE

www.kaspersky.de

Checklist: Wie man seine Daten online schützt

Fotos, hochgeladene Dokumente oder App-Details – Datenmanagement ist Teil unseres Alltags, ob wir uns dessen bewusst sind oder nicht. Aber wissen wir, wo unsere Daten landen, und könnten sie in die falschen Hände geraten? Wir müssen lernen, wie wir mit personenbezogenen Daten verantwortungsvoll umgehen und diese teilen können – egal, ob es sich dabei um Daten handelt, die wir selbst oder Dritte managen. Hinzu kommen Daten von anderen, auf die wir Zugriff haben. Diese Checkliste zeigt, wie man die Kontrolle über die eigenen Daten behalten kann.

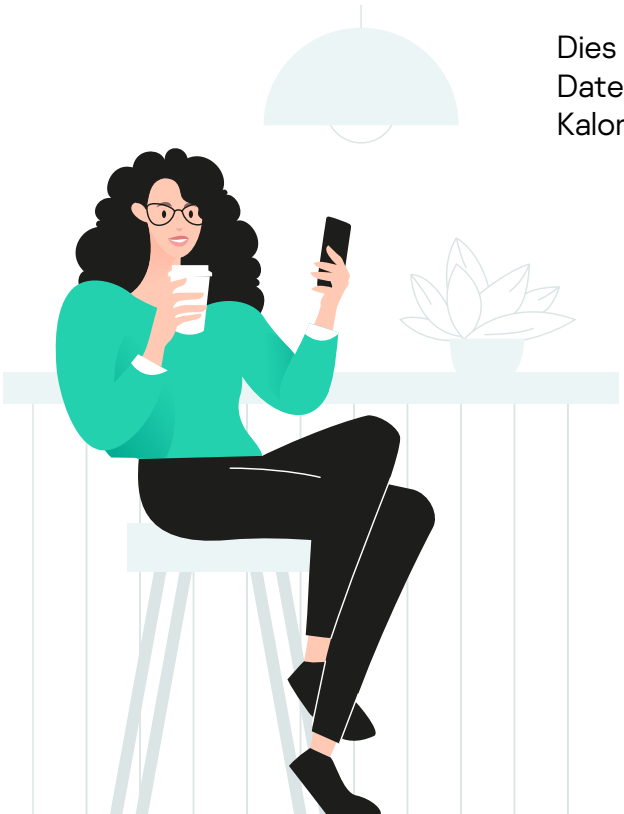
Informationen über Dich, die Du kontrollieren kannst

1.

Sei Dir bewusst, welche persönlichen Daten Du mit wem teilst und inwiefern Du diesen Dritten vertrauen kannst

Wenn Du persönliche Daten, mit denen Du identifiziert werden kannst (Reisepässe, Personalausweise, Krankenversicherungen), weitergibst, vergewissere Dich, dass Du weißt, an welchen Dienst oder welche Person Du diese Daten sendest. Vergewissere Dich auch, ob Du diesem bestimmten Dienst oder dieser Person vertrauen kannst. Prüfe bei Unternehmen, ob es in der Vergangenheit bereits eine Datenverletzung gegeben hat. Denke jedes Mal nach, bevor Du Dokumente digital an andere weitergibst.

Dies ist besonders wichtig, wenn es um das Teilen medizinischer Daten geht (beispielsweise Menstruationszyklus, Blutzucker, Kalorienverbrauch etc.).



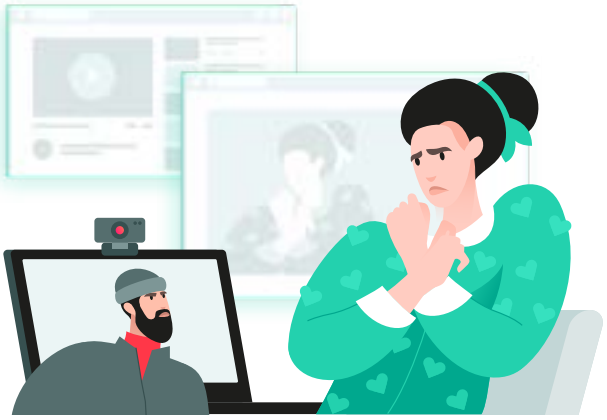
2.

Achte darauf, mit wem Du Deine Daten teilst – und wann Du das tust

Du solltest den Überblick darüber behalten, mit welchen Dritten Du persönliche Daten geteilt hast. Denn so kannst Du bei einem bekannt gewordenen Datenleck überprüfen, ob Deine Daten möglicherweise kompromittiert wurden. Hierbei kann ein Passwort-Manager helfen, in dem alle Dienste, bei denen man sich registriert hat, gespeichert sind. Wenn Du persönliche Informationen teilst, überlege zwei Mal, ob Du das tun möchtest.

Weitere Informationen:

Herausfinden, welche Daten Apps wirklich sammeln



3.

Denke nach, bevor Du etwas postest – die Informationen verbleiben oft im Internet, auch wenn das Profil gelöscht wurde

Auf der Grundlage Deiner Beiträge in Sozialen Netzwerken kann ein „soziales Profil“ erstellt und gegen Dich verwendet werden. Kannst und willst Du für alles, was Du je online geäußert hast, gerade stehen? Ziehe in Erwägung, Dein Konto in den Privat-Modus zu schalten, aber sei Dir auch bewusst, dass es dadurch nicht vollständig verborgen ist; es gibt immer noch eine Reihe von Möglichkeiten, dass Deine geposteten Beiträge öffentlich werden (zum Beispiel, wenn Deine Follower gehackt werden).

Weitere Informationen

Datenschutzeinstellungen für Online-Dienste anpassen
Schütze Deine Privatsphäre online
Die Kontrolle über die eigenen Daten übernehmen

4.

Verwende, wenn überhaupt, abstrakte Geotags. Markiere keine Fotos mit bestimmten Orten, die Du regelmäßig besuchst

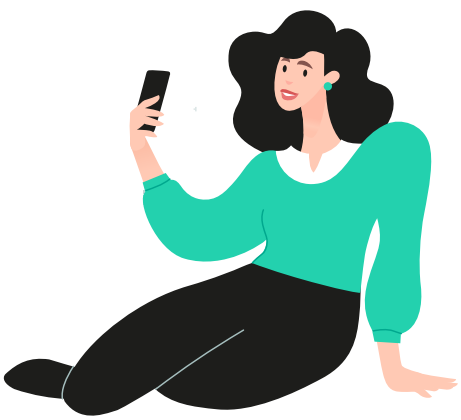
Geolokalisierung ist eine der sensibelsten Art von Daten, durch die Du kompromittiert werden kannst. Denn durch Geotags können Cyberkriminelle herausfinden, wo Du wohnst, wo Du dich aufhältst, welche Routen Du nimmst und wann Du nicht zu Hause bist. Das Teilen der Geotags von Orten hingegen, an die Du reist oder die Du selten besuchst, ist im Allgemeinen sicherer.

Richte Deine Datenschutzeinstellungen für soziale Medien mit Hilfe des Kaspersky Privacy Checker ein.

5.

Achte darauf, dass keine persönlichen Daten auf geteilten Fotos zu finden sind

Das klingt zunächst einfach und selbstverständlich, doch wenn man sich die Hashtags #tickets oder #flights anschaut, sieht man, dass immer noch viele persönliche Daten auf Fotos teilen – zum Beispiel Flugbuchungsnummern auf einer Bordkarte. Jedes Mal, wenn diese Art von Daten öffentlich gemacht wird, besteht die Gefahr des Missbrauchs. Tatsächlich gab es bereits den Fall, dass jemand den Flug eines ahnungslosen Nutzers zum Spaß storniert hat, indem er die Fluggesellschaft mit der online veröffentlichten Buchungsnummer und dem Namen des Nutzers anrief. Wenn Du etwas über Deine Reisen mitteilen möchtest, achte darauf, dass die Fotos keine persönlichen Daten enthalten.



Weitere Informationen:
Unerwünschte Informationen auf Bildern richtig verbergen

6.

Erkenne, welche Messenger sicher sind und welche eine Ende-zu-Ende-Verschlüsselung nutzen

Persönliche Unterhaltungen, die in der Regel in Messenger-Apps stattfinden, gehören zu den sensibelsten Daten von allen. Wir nutzen Messenger, um uns über private und wichtige Themen auszutauschen – Dinge, die unsere Schwächen oder wunden Punkte aufzeigen können. Daher ist es entscheidend zu wissen, wie sicher der verwendete Messenger ist und welche Art von Daten – Text oder Fotos – mit geringem Risiko ausgetauscht werden können. Bringe in Erfahrung, ob Deine genutzten Messenger-Apps Nachrichten auf dem Gerät, in einer Cloud oder auf einem Server speichern, von wo aus sie geleakt werden können. Denke außerdem an weitere Datenschutzoptionen, beispielsweise ob die App Dich informiert, wenn der Teilnehmer einer Konversation einen Screenshot von Eurer Kommunikation gemacht hat, oder versucht, Nachrichten zu versenden, die sich selbst löschen.

Weitere Informationen:

Telegram - Tipps für Privatsphäre und Sicherheit
Was eine Ende-zu-Ende-Verschlüsselung ist und warum man sie benötigt

7.

Investiere klug in Smart Devices. Billige Entwicklung bedeutet oft höheres Risiko für Datenlecks

Fitness-Tracker und Smartwatches, die wir rund um die Uhr tragen, sind alle mit Apps verbunden, die biometrische Daten sammeln. Es gibt zwar viele günstige Geräte, aber sei Dir bewusst: Je weniger der Entwickler in das Gerät und die App investiert hat, desto geringer wird das Sicherheitslevel sein. Die Grundregel lautet: In die Kaufentscheidung sollten Preis, Popularität des Geräts und Nutzerfreundlichkeit der Anwendung, mit der dieses funktioniert, miteinfließen. Informiere Dich also vor dem Kauf über die Anwendung, mit der ein Tracker verknüpft werden soll, und prüfe, ob es in der Vergangenheit bereits Datenlecks gegeben hat. Des Weiteren können Nutzerbewertungen herangezogen werden. Das Gleiche gilt für Smartphones, Videokameras und Babyphones.

8.

Kaufe nur bei vertrauenwürdigen Händlern ein

Die Menge an Online-Shops, die mehr oder weniger das Gleiche anbieten, kann uns verwirren. Aber alle Geschäfte haben unterschiedliche Datenschutzrichtlinien, einige auch – gar keine. Je weniger Online-Shops man nutzt, desto weniger Informationen gibt man weiter.

Informationen über Dich, über die Du keine Kontrolle hast

Browser-Aktivität

Jeder einzelne Schritt, den Du im Browser machst, wird durch Cookies und Tracking-URLs nachvollzogen. Darüber hinaus gibt es unzählige Fingerprinting-Mechanismen, die zur eindeutigen Identifizierung eines Nutzers im Internet verwendet werden. Diese Daten ermöglichen es Unternehmen, ein detailliertes Profil zu erstellen – zweifelsohne auch, um Werbung zu streuen und das Nutzererlebnis zu verbessern. Aber das hat seinen Preis: Diese Daten sind angreifbar. Es liegt also an Dir, die richtige Balance zwischen Privatsphäre und einer verbesserten Nutzererfahrung zu finden.

1.

Entscheide Dich für einen Browser, der Datenschutz berücksichtigt – oder nutze Plug-ins, die das Tracking minimieren

Es gibt Tracking-URLs, die zu Werbezwecken parallel zu dem Tracking, das von der Webseite ausgeführt wird, geladen werden, um zusätzliche Aktivitäten zu verfolgen. Installiere daher vertrauenswürdige Datenschutz- und Sicherheits-Add-ons wie Tracker-Blocker, Werbeblocker und Sicherheitstools und verwende Plug-ins, die Tracking-Links verhindern. Kaspersky-Produkte verfügen zum Beispiel über eine Do-Not-Track-Komponente, die das Laden von Tracking-Elementen verhindert, mit denen das Nutzerverhalten auf Websites aufgezeichnet wird.

Weitere Informationen:
Wie man erkennt, ob eine Website (Browser-) Fingerabdrücke nimmt

2.

Einstellungen so konfigurieren, dass Browser-Cookies nach jeder Sitzung gelöscht werden

In den Einstellungen des Browsers können die Cookie-Aktivitäten begrenzt werden. Dadurch lassen sich Deine Web-Aktivitäten nicht langfristig nachverfolgen und Du verhinderst, dass diese ein definiertes Profil von Dir erstellen. Hier solltest Du den Unterschied zwischen Erstanbieter- und Drittanbieter-Cookies beachten: Erstanbieter-Cookies dienen dazu, das Nutzererlebnis zu verbessern, das Surfen bequemer zu machen und personalisierte Empfehlungen zu geben. Sie sind im Allgemeinen sicher. Zusätzlich jedoch verfolgen Cookies von Drittanbietern dieselbe Aktivität oder die interessantesten Aktivitäten, um ein Profil von Dir zu erstellen und Werbung zu personalisieren – sie können auch Deinen Browserverlauf verfolgen. Einige Browser, wie zum Beispiel Safari, haben inzwischen standardmäßig eine robustere Datenschutzrichtlinie in Bezug auf Cookies implementiert.

Weitere Informationen:
Dimensionen des Web-Trackings verstehen

3.

Optimiere die Datenschutzeinstellungen in den Optionen Deines Browsers

Wenn Du etwas Aufwand für den Schutz Deiner Daten in Kauf nehmen möchtest, sowohl aus Sicht des Datenschutzes als auch der Sicherheit, solltest Du zusätzliche Maßnahmen in Betracht ziehen. Zum Beispiel bietet Firefox Containers eine Option für Nutzer, Teile ihrer Online-Aktivitäten sorgfältig in separate Boxen zu segmentieren, die die für diese Segmente relevanten Daten voneinander getrennt halten. Weitere Optionen wären, einzuschränken, welche Websites Zugriff auf Standortdaten, Mikrofon und Webcam haben, und sogar, welche Websites JavaScript aktiviert haben.

Technologie-affine Nutzer können in Erwägung ziehen, die WebRTC-APIs zu deaktivieren, wenn das potenzielle Durchsickern Ihrer IP-Adresse ein Grund zur Sorge ist. Eine weitere Option, die normalerweise in den meisten Browsern automatisch aktiviert ist und die viele Nutzer aus Sicherheitsgründen deaktivieren möchten, ist das automatische Speichern und Ausfüllen von Kennwörtern. Wenn der Browser dies unterstützt, solltest Du den „Nur-HTTPS-Modus“ aktivieren, der automatisch versucht, den gesamten HTTP-Verkehr auf Websites zu verschlüsseln (der größte Teil des Webs verwendet inzwischen glücklicherweise HTTPS, aber es gibt immer noch Ausreißer, und es ist besser, auf Nummer sicher zu gehen).

Viele dieser Aufgaben können mit Hilfe von Browser-Erweiterungen wie Privacy Badger automatisch erledigt werden. Dieses Projekt wird von der Electronic Frontier Foundation (EFF) betreut und ist ein kostenloses, installierbares Browser-Add-on, das im Hintergrund in den Browsern der Nutzer arbeitet, um sie zu höheren Datenschutzeinstellungen anzuhalten.

4.

Inkognito-Modus beim Surfen im Internet verwenden

Wenn Du nach etwas im Internet suchen möchtest, aber nicht willst, dass es in Deinem Verlauf gespeichert wird, solltest Du den Inkognito-Modus des Browsers verwenden. Damit wird eingeschränkt, dass der Browserverlauf zurückverfolgt wird; des Weiteren werden alle Cookies deaktiviert, was die Suche privat macht. Dies ist besonders nützlich, wenn Du Deinen Computer mit anderen teilst.

Weitere Informationen:

Q&A Inkognito-Modus

Tracking durch Apps

Mobile Apps verfolgen und sammeln Daten auf die gleiche Weise wie Webbrowser. Zusätzlich tragen wir Smartphones überall mit uns herum, sodass diese viel mehr über uns wissen, als wir vielleicht vermuten. Es gibt zwei Möglichkeiten, das Sammeln von Daten durch mobile Geräte einzuschränken. So geht's:

5.

Verwende einen VPN-Dienst

Ein VPN verschlüsselt den Datenverkehr Deines Geräts vollständig und schützt ihn vor dem Zugriff Dritter, auch vor dem Provider, selbst wenn Du in einem öffentlichen WLAN-Netz unterwegs bist. Ein VPN kann einige Informationen über Dich und Dein Gerät ändern (beispielsweise die IP-Adresse) und es damit für Unternehmen schwieriger machen, Dich aufzuspüren. Es ist wichtig zu bedenken, dass ein VPN auch Nutzerdaten sammelt. Daher sollte man einen Dienst wählen, dem man vertraut. Die kostenlose Version eines VPNs reicht zwar aus, um den Datenverkehr vor einem Provider zu verbergen, der Hersteller kann den Verkehr aber trotzdem an Dritte verkaufen. Wähle daher einen Dienst von einem angesehenen Anbieter mit einer Erklärung zur Datenverarbeitung, zum Beispiel Kaspersky Secure Connection.

Weitere Informationen:

So schützt man sein WLAN Zuhause
Wie man einen VPN-Dienst auswählt

6.

Ändere die Standortinformation auf Deinem Telefon

Wenn Du die Tracker über Deinen Standort täuschst, stiftest Du Verwirrung und erschwerst damit die Erstellung eines detaillierten Profils. Richte daher ein anderes regionales Gebietsschema auf Deinem Betriebssystem ein und wähle ein Drittland für die VPN-Verbindung. Wähle zum Beispiel die deutsche Version des iOS und eine finnische VPN-Verbindung. Die Änderung der Standortangabe kann allerdings dazu führen, dass beispielsweise Zahlungsdienste nicht funktioniert, weil der Dienst in dem gewählten Land nicht unterstützt wird. Wechsle in solchen Fällen einfach zurück in Dein eigentliches Land, nimm die Zahlung vor und wechsle danach zurück in ein Land Deiner Wahl.

7.

Zugriffseinstellungen für jede Anwendung auf Deinem Telefon spezifisch einrichten

Verwende Funktionen, die die Betriebssystementwickler erstellt haben, um sicherzustellen, dass Anwendungen nur auf die Informationen zugreifen können, die sie benötigen. Zu den bewährten Praktiken zählen, den Zugriff auf Deinen Standort nur während der Verwendung einer App zuzulassen und den Zugriff auf das Mikrofon und Fotos zu beschränken. Sei vorsichtig mit Anwendungen, die Daten anfordern, die sie nicht benötigen, um ihre eigentlichen Funktionen auszuführen.

Weitere Informationen:

Mit Off-Facebook-Aktivitäten haben Sie (etwas) Kontrolle über Ihre Daten

Aktualisierte Sicherheits- und Privatsphäre-Einstellungen bei Instagram

8.

Niemals nicht verifizierte Anwendungen installieren

Nicht verifizierte Anwendungen (Apps, die den Verifizierungsprozess eines App-Stores nicht durchlaufen haben) sind oft Adware – eine Art von Software, die das Telefon mit Werbung überflutet und Metadaten sammelt. Noch schlimmer: Die App, die man herunterlädt, könnte schädlich sein und beispielsweise Spyware enthalten, die Informationen über Deinen Standort, Deine Unterhaltungen in Messengern oder Anrufprotokolle sammelt.

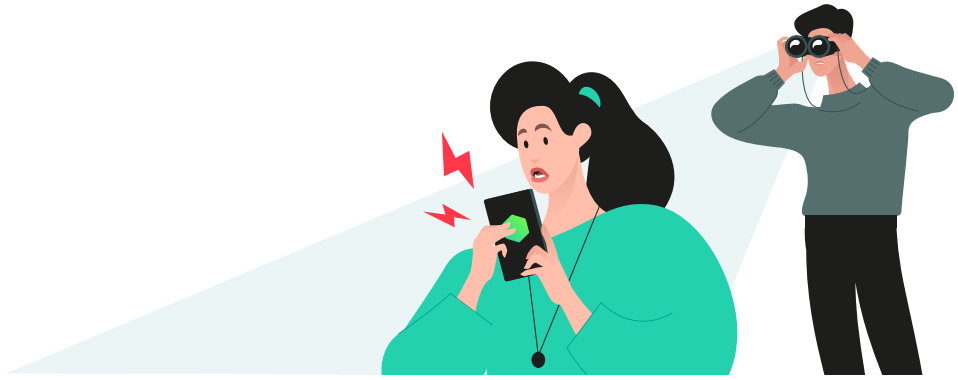
Informationen zu anderen Personen, über die Du die Kontrolle hast

Ob Fotos von anderen Personen, Unterhaltungen, Chats, Telefonnummern oder Adressen – Du hast oft Zugang zu persönlichen Informationen anderer Menschen. Auch mit diesen muss verantwortungsvoll umgegangen werden und Du musst diese sicher aufbewahren. So geht's:

1.

Gib persönliche Informationen nur mit Zustimmung der betroffenen Personen weiter

Fotos von anderen Menschen, die Du aufgenommen hast, können von Dir als harmlos angesehen werden, könnten diesen aber schaden. Das Gleiche gilt für Screenshots von Gesprächen, gemeinsam gekauften Flugtickets usw. – also so ziemlich für alles, was Informationen über eine dritte Person enthält und diese identifizieren könnte. Denke daran, dass Du nicht nur Verantwortung für Deine eigenen Daten trägst, sondern auch für die Daten anderer, die zufällig zu den Deinen geworden sind.



2.

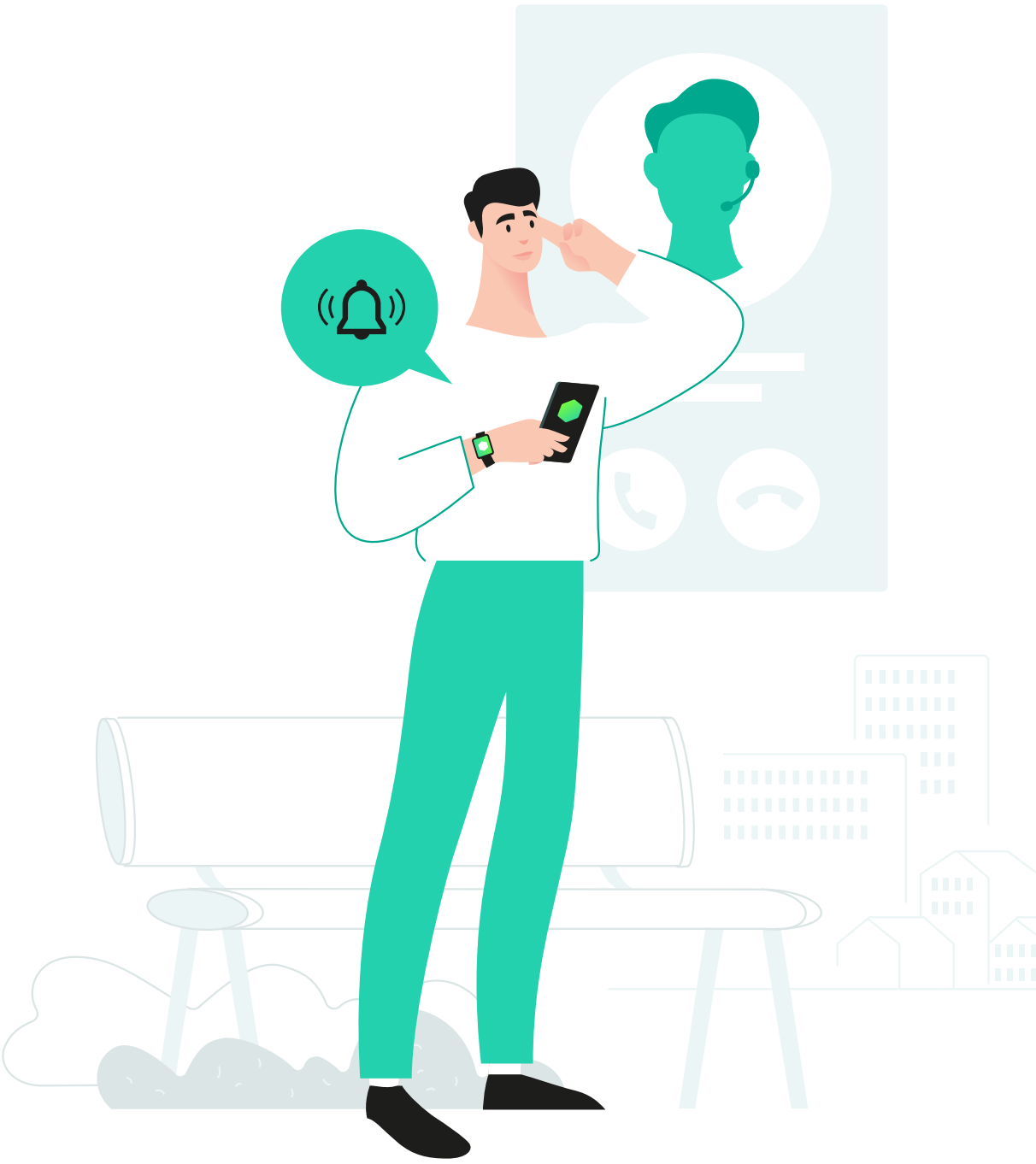
Behandle die persönlichen Daten anderer Personen als wären es Deine eigenen

Befolge bei den Daten anderer Personen die gleichen Grundsätze wie bei Deinen eigenen Daten. Lade personenbezogene Daten von Dritten nur in zuverlässige Quellen hoch, zeige diese nicht anderen Personen und berücksichtige, wie diese Daten verwendet werden könnten.

3.

Weise andere daraufhin, wenn Du ein Gespräch aufnimmst

Abgesehen davon, dass heimliche Ton- und Videoaufnahmen generell unethisch und respektlos gegenüber den Gesprächsteilnehmern sind, ist dies in einigen Ländern auch verboten.



4.

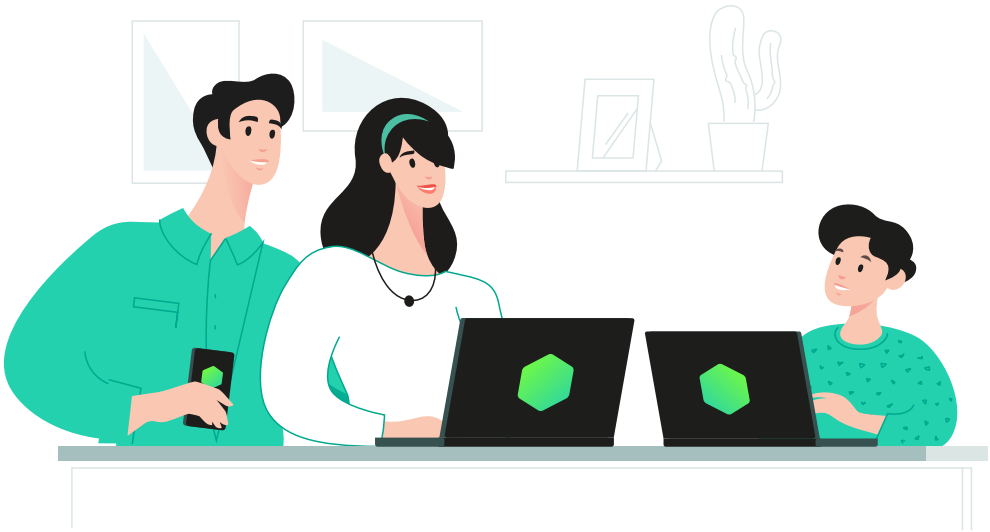
Teile keine Informationen über Familienangehörige oder Nahestehende auf öffentlich-zugänglichen Social-Media-Konten

Persönliche Verbindungen verraten mehr, als man denken könnte – sie zeigen, welche Menschen einem viel bedeuten und machen Dich dadurch verletzlich. Diese Informationen können nicht nur gegen Dich, sondern auch gegen diejenigen verwendet werden, die Dir nahestehen.

5.

Spreche mit Deinen Freunden und Deiner Familie über Datenschutz

Tausche Dich mit Deinen Nächsten aus, um gegenseitige Regeln und Standards für die Datenhygiene zu vereinbaren. Man sollte sich gegenseitig informieren, falls und wenn etwas im Zusammenhang mit persönlichen Datenlecks passiert. Innerhalb Deines persönlichen Netzwerks sollte im Hinblick auf die Weitergabe von Daten nach außen ein gutes Maß an Vertraulichkeit gegeben sein.



www.kaspersky.de

kaspersky

GBD-7837 Q1/21 V1