Lerneinheit

[Smartphone- Schutz]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

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

Das Thema

Einführung

Social Media, Instant Messenger, Shopping, Spiele, Apps, schnell ein Foto machen oder googeln - viele Menschen können sich den Alltag ohne ihr Smartphone kaum noch vorstellen. Zum Telefonieren wird es jedoch immer weniger genutzt. Der klare Trend geht zum Tippen statt zum Telefonieren. Dies zeigt auch ein Blick auf die Zahl der NutzerInnen von Instant-Messenger-Diensten: Rund 1,6 Milliarden Menschen weltweit nutzen WhatsApp, und etwa 1,3 Milliarden kommunizieren mit ihren Freunden über Facebook Messenger. Die Nutzung dieser Dienste ist ein Kinderspiel. Doch welche Gefahren lauern bei der Nutzung von Instant Messenger-Diensten oder anderen Smartphone-Anwendungen im Hinblick auf den Datenschutz? Nicht umsonst werden Facebook oder andere AnbieterInnen von kostenlosen Smartphone-Anwendungen immer wieder von DatenschützerInnen kritisiert. Finden Sie heraus, wie Sie Ihr Smartphone, Ihre Daten und Ihre Privatsphäre besser schützen können!

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Nach Abschluss dieser Lerneinheit werden Sie in der Lage sein, die mit der Nutzung von Instant-Messaging-Diensten oder anderen Smartphone-Apps verbundenen Risiken besser einzuschätzen, und Sie werden einige nützliche Schritte kennenlernen, um Ihr Telefon und Ihre Privatsphäre vor unerwünschten Risiken zu schützen.

1.Wissen aufbauen - Grundlegende Schutzmaßnahmen für Smartphones

Für viele Menschen ist ihr Smartphone ihr ständiger Begleiter im Alltag. Gehören auch Sie zu denjenigen, die ihr Smartphone überall hin mitnehmen und nicht einen Tag lang darauf verzichten können? Wenn ja, dann haben Sie wahrscheinlich auch sehr private oder sensible Daten auf Ihrem Smartphone, wie zum Beispiel Fotos, vertrauliche Textnachrichten oder Geschäftsinformationen. Um Ihr Smartphone und

die darin gespeicherten, möglicherweise sehr privaten Daten zu schützen, sollten Sie bei Verlust oder Diebstahl geeignete Maßnahmen ergreifen.

Dazu gehört zum Beispiel der Schutz des Smartphones vor unbefugtem Zugriff mittels PIN (Personal Identification Number) und Bildschirmsperre.

Wichtig
Stellen Sie sicher, dass Sie **keine üblichen Zahlenkombinationen** wie "1234", "1111" oder ähnliche verwenden. Diese sind sehr leicht von Unbefugten zu hacken.

Wenn Ihr Smartphone gestohlen wird oder verloren geht, sollten Sie die **SIM-Karte** (Subscriber Identity Module) des Geräts von Ihrem Netzbetreiber **sperren** lassen, damit niemand damit telefonieren oder hohe Kosten verursachen kann.

Kennen Sie die **Seriennummer Ihres Smartphones**? Diese befindet sich unter dem Akku, auf der Originalverpackung oder auf der Rechnung für den Kauf des Mobiltelefons. Sie sollten sich **diese Nummer notieren**, damit Sie sie im Falle eines Diebstahls bei der Polizei melden können.

Alle gängigen Betriebssysteme bieten auch **verschiedene Dienste** an, die im Falle eines Diebstahls oder Verlusts sehr hilfreich sein können.

Beispiele
Können Sie Ihr Mobiltelefon nicht finden? Mit dem **Android Device Manager** können Sie Ihr Smartphone mit maximaler Lautstärke klingeln lassen, auch wenn es stumm geschaltet war. Auf diese Weise können Sie ein verlorenes Telefon zu Hause schnell wiederfinden. Wenn es woanders ist, können Sie es in Echtzeit lokalisieren und dem Finder/ der Finderin eine Nachricht hinterlassen. Wenn Ihr iPhone verloren gegangen ist oder gestohlen wurde, können Sie es normalerweise über **iCloud** suchen, vorausgesetzt, das Gerät ist eingeschaltet und hat Datenempfang.

Wahrscheinlich haben Sie bereits von der Möglichkeit gehört, eine Art Anti-Diebstahl-Anwendung auf Ihrem Smartphone zu installieren. Sie ermöglicht es Ihnen beispielsweise, das verlorene oder gestohlene Smartphone zu lokalisieren, zu sperren und die darauf gespeicherten Daten zu löschen. Die

dafür erforderlichen Befehle können von einem anderen Smartphone, dessen Nummer gespeichert ist, erteilt oder über ein Online-Portal an das Gerät gesendet werden.

Tipp
Im Falle von Diebstahl oder Verlust sollten Sie die SIM-Karte sofort sperren, wenn Sie **keine Anti-Diebstahl-App auf Ihrem Telefon installiert haben**. Wenn jedoch eine App installiert ist, sollte die SIM-Karte erst dann gesperrt werden, wenn die Daten lokalisiert und aus der Ferne gelöscht wurden. Andernfalls ist dies nicht mehr möglich.

1.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche Maßnahmen können Sie ergreifen, um Ihr Smartphone vor unberechtigtem Zugriff zu schützen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Ich kann eine PIN verwenden. Diese PIN sollte so einfach wie möglich zu merken sein.
- Ich sollte mein Smartphone mit einer PIN sperren und sicherstellen, dass es sich nicht um eine Zahlenkombination wie 1234 oder 1111 handelt.
- Ich kann eine Bildschirmsperre einrichten.
- Ich kann eine kostenpflichtige Anwendung installieren, um eine persönliche Identifikationsnummer einzurichten.

Übung MULTIPLE CHOICE

Situation: Nach einem Einkaufsnachmittag in der Stadt stellen Sie zu Hause plötzlich fest, dass Sie Ihr Smartphone verloren haben. Welche Maßnahmen können in einer solchen Situation sinnvoll sein?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Ich kann den Android Device Manager oder die iCloud verwenden, um mein Smartphone zu lokalisieren.
- Ich kann eine Art Anti-Diebstahl-App für solche Fälle installieren. Damit kann ich mein Telefon lokalisieren, sperren oder gespeicherte Daten auf dem Telefon löschen.
- Ich kann meine SIM-Karte sperren lassen, damit ich mein Telefon lokalisieren kann.
- Ich kann meine SIM-Karte sperren lassen, um zu verhindern, dass jemand durch die Benutzung meines Telefons hohe Kosten verursacht.

2.Wissen aufbauen - Instant Messaging (IM) und Anwendungen

Die Möglichkeit, Textnachrichten über das Mobiltelefon auszutauschen, ist nicht neu. In den letzten Jahren wurde jedoch aufgrund der weit verbreiteten Nutzung von Smartphones die Kommunikation über SMS zunehmend durch die Nutzung von **Instant-Messaging-Diensten (IM)** ersetzt.

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

Definition
Im Gegensatz zu SMS-Diensten handelt es sich bei **IM** um eine **internetbasierte Kommunikation über mobile Apps**. Es handelt sich dabei um eine Art Online-Chat, der es Ihnen ermöglicht, Nachrichten mit anderen BenutzerInnen nahezu in Echtzeit auszutauschen. Dazu müssen Instant-Messaging-Anwendungen heruntergeladen und installiert werden.

Neben der Übertragung von Texten ist in der Regel auch die Übertragung von Dateien, Audio- und Videosequenzen (und damit auch Video-Chat) möglich. Die Nachrichtenübermittlung erfolgt im sogenannten **Push-Verfahren**, wodurch die Texte unmittelbar nach dem Versenden beim Empfänger bzw. bei der Empfängerin ankommen. Anders als z.B. bei E-Mails müssen die Nachrichten nicht erst abgerufen werden, sondern erscheinen sofort auf dem Bildschirm des Kommunikationspartners.

Beispiel:
Beispiele für beliebte Instant-Messaging-Dienste: • Windows Life Messenger • Skype • Facebook Messenger • WhatsApp • WeChat • Telegramm

Beispielsweise nutzen weltweit bereits rund 1,3 Milliarden NutzerInnen den Facebook Messenger zur Kommunikation.

Die häufigste Nutzung von Instant-Messaging-Programmen erfolgt auf mobilen Geräten wie **Smartphones** über **Messenger-Apps**. Messenger-Apps sind in der Regel kostenlos, praktisch, einfach zu bedienen und erfreuen sich daher zunehmender Beliebtheit. Um z.B. WhatsApp zu nutzen, müssen Sie nur die kostenlose App herunterladen und sich über Ihre eigene Mobiltelefonnummer registrieren.

Um den gewünschten Zweck zu erfüllen, benötigt eine App jedoch in der Regel eine Vielzahl von **Berechtigungen**. Daher möchte die App auf bestimmte Gerätefunktionen Ihres Smartphones zugreifen, wie z.B. Kalender, Kamera, Kontakte, Mikrofon, SMS, Speicher, Standort oder Telefonfunktion.

Wichtig
Gehören Sie zu den 1,6 Milliarden WhatsApp-NutzerInnen weltweit? Dann sollten Sie sich bewusst sein, dass WhatsApp zumindest auf alle **Kontaktadressen** zugreift, die **auf Ihrem Mobiltelefon** gespeichert sind.

Nur so kann die App feststellen, welcher Ihrer Kontakte ebenfalls WhatsApp verwendet, und diese automatisch in der App anzeigen. Möchten Sie Bilder oder Ihren eigenen Standort über WhatsApp versenden oder für Videotelefonie nutzen? Dann sollten Sie sich bewusst sein, dass WhatsApp auch auf Ihre Bilder, Kamera-, Mikrofon- und Standortdaten zugreifen muss!

Tipp
Aus Datenschutzgründen lohnt es sich, bei der Vergabe von **Berechtigungen an Apps** vorsichtig vorzugehen und die Berechtigungen auf das notwendigste Maß zu reduzieren.

Wenn Sie sich nicht sicher sind, welche Berechtigung jede App auf Ihrem Smartphone hat, sollten Sie dies aus Sicherheitsgründen überprüfen. Fragen Sie sich, wie Sie das machen können? Wählen Sie einfach die entsprechende App unter "Einstellungen" aus, sehen Sie nach, welche Zugriffe Sie der App erlauben und passen Sie diese gegebenenfalls an.

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

Beispiel

Angenommen, Sie möchten Google Maps verwenden, um eine bestimmte Adresse zu finden. In diesem Fall ist es sinnvoll, der App zu erlauben, auf Ihren Standort zuzugreifen, während Sie die App verwenden. Wenn Sie Ihren Standort jedoch nicht über WhatsApp für Ihre Kontakte freigeben möchten, muss die App nicht unbedingt wissen, wo Sie sich befinden.

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

2.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen über Instant Messaging (IM)-Dienste sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- Immer mehr Menschen nutzen IM-Dienste zum Austausch von Textnachrichten, während die Kommunikation per SMS an Beliebtheit verloren hat.
- IM ist Internet-basierte Kommunikation.
- IM ermöglicht nicht nur den Austausch von Textnachrichten, sondern auch den Austausch von Dateien, Audios oder die Kommunikation über Video-Chat.
- Wenn viele Menschen gleichzeitig beliebte IM-Dienste nutzen, dauert es in der Regel einige Minuten, bis der Empfänger die Nachrichten erhält.
- Beliebte IM-Dienste sind Facebook Messenger, WhatsApp oder Windows Life Messenger.
- Beliebte IM-Dienste sind Youtube, Twitter, WhatsApp und Google.

Übung MULTIPLE CHOICE

Situation: Sie möchten WhatsApp verwenden, um mit Ihren Freunden zu kommunizieren. Was sollten Sie bei der Installation der App beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Messenger-Apps wie WhatsApp erfordern in der Regel die einmalige Zahlung einer Nutzungsgebühr im Voraus.
- Um WhatsApp nutzen zu können, müssen Sie die Anwendung herunterladen und sich mit Ihrem echten Namen registrieren.
- WhatsApp greift auf alle in Ihrem Smartphone gespeicherten Kontakte zu.
- Um bestimmte Dienste von WhatsApp nutzen zu können, kann es erforderlich sein, der App den Zugriff auf Ihre Bilder, Kamera, Mikrofon oder Standortdaten zu erlauben.
- WhatsApp greift automatisch auf alle in Ihrem Smartphone gespeicherten Kontakte, Ihre Bilder und Ihre Standortdaten zu. Dies ist die einzige Möglichkeit, wie die App funktionieren kann.

Übung MULTIPLE CHOICE

Situation: Wann ist es sinnvoll, App-Berechtigungen anzupassen und wie ist dies grundsätzlich möglich?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Grundsätzlich können Sie unter "Einstellungen" leicht überprüfen, welche der installierten Apps welche Zugriffsrechte besitzen und diese ggf. auf das wirklich notwendige Maß reduzieren.
- Um herauszufinden, welche Zugriffsrechte eine App hat, ist es ratsam, Ihren Mobilfunkanbieter anzurufen.
- Wenn Sie z.B. Google Maps verwenden möchten, ist es sinnvoll, der App den Zugriff auf Ihre Standortdaten zu erlauben, während Sie die App benutzen.
- Es ist auch eine gute Idee, WhatsApp den Zugriff auf Ihre Standortdaten zu gestatten, da dies dazu beiträgt, dass Ihre Nachrichten schneller übertragen werden.
- Da die meisten Apps kostenlos sind, ist es in der Regel nicht möglich, die Zugriffsrechte der Apps einzeln einzuschränken.

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

3.Wissen aufbauen - Sicherheitsrisiken durch Smartphone-Anwendung

Wenn Sie auf Ihrem Smartphone auch viele Daten zum Teil sehr privater Natur und von Dritten (z.B. Fotos) speichern und verarbeiten, sollten Sie überlegen, inwieweit **uneingeschränkte App-Berechtigungen** problematisch sein könnten.

Es ist kein Geheimnis, dass viele App-ProduzentInnen an Ihren persönlichen Daten interessiert sind. Schließlich müssen sie mit den Apps, die den NutzerInnen oft kostenlos zur Verfügung gestellt werden, in irgendeiner Form Einnahmen erzielen. **Wenn Sie für ein Produkt nicht bezahlen, dann sind Sie in der Regel das Produkt**, heißt es. Aber das ist noch kein Grund zur Besorgnis. In den meisten Fällen wird die Verwendung unserer persönlichen Daten im Rahmen der gesetzlichen Datenschutzbestimmungen anonymisiert.

Durch die **Übernahme von WhatsApp durch z.B. Facebook** werden aber auch die Telefonnummern aus dem Kontaktverzeichnis an Facebook weitergegeben. Darüber hinaus hat die Aufdeckung verschiedener Vorfälle im Bereich des Datenschutzes in der Vergangenheit auch zu einer Sensibilisierung für die Gefahren einer unberechtigten Überwachung geführt. Die NutzerInnen machen sich zunehmend Sorgen um den Datenschutz.

Fragen Sie sich nun, welche Sicherheitsprobleme und unerwünschten Folgen die Nutzung von Instant-Messaging-Diensten und anderen Anwendungen für Sie haben kann? Hier sind einige Beispiele:

- Wie bei anderen Online-Kommunikationsmedien besteht auch bei Messengern das Risiko, **Phishing-Links zu versenden oder Schadsoftware** über anklickbare Hyperlinks oder übertragene Dateien zu übertragen.
- Es besteht die Gefahr, dass sich **in den Apps Malware aller Art versteckt**, insbesondere wenn Apps kostenlos im Internet bei weniger seriösen App-AnbieterInnen gekauft wurden.
- Wie Sie bereits wissen, erhalten Apps Berechtigungen zur Ausführung von Funktionen. Die Berechtigungen erlauben es den Apps, Daten zu lesen. Es besteht also die Gefahr eines **versteckten Zugriffs auf persönliche Daten** wie Standortdaten, mobile Surfgewohnheiten, gespeicherte Kontaktdaten oder Passwörter. Neben dem Verlust der Privatsphäre kann auch der **Missbrauch Ihrer Kontaktdaten** eine unangenehme Folge sein.

- **Probleme mit dem Urheberrecht** können z.B. entstehen, wenn Bilder, die Sie nicht selbst erstellt haben und für die Sie nicht das Urheberrecht besitzen, als Profilfotos verwendet werden.
- **Unverschlüsselte Kommunikation** stellt ein hohes Sicherheitsrisiko dar. Deshalb werden seit April 2016 Inhalte, die z.B. über WhatsApp gesendet werden, mit einer sicheren Ende-zu-Ende-Verschlüsselung übertragen. Dies gilt für Texte, Bilder, Videos und andere Dateien. Ende-zu-Ende-Verschlüsselung bedeutet, dass nur die jeweiligen KommunikationspartnerInnen die Inhalte empfangen und lesen können.

Wichtig
Wenn Sie die Facebook Message App verwenden, sollten Sie beachten, dass Ihre Kommunikation (im Gegensatz zu WhatsApp) grundsätzlich nicht verschlüsselt ist! Wenn Sie Ende-zu-Ende-verschlüsselt chatten möchten, müssen Sie eine "geheime Konversation" starten. Wie dies funktioniert, wird in der nächsten Session erläutert.

3.Wissen anwenden

Übung SINGLE CHOICE

Situation: Warum sind die NutzerInnen von Apps zunehmend besorgt über den Datenschutz?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Weil Apps von immer mehr Menschen genutzt werden
- Weil die Apps in erster Linie von Unternehmen entwickelt werden, die in Ländern ansässig sind, die sich nicht um den Datenschutz kümmern, und es daher keine verbindlichen Datenschutzregeln für den Umgang mit Benutzerdaten gibt. Ein bekanntes Beispiel ist Facebook oder WhatsApp.
- Weil die Apps immer teurer werden.
- Weil in den letzten Jahren einige Datenschutzverletzungen bekannt geworden sind.
- Weil es für BenutzerInnen nicht nachvollziehbar ist, welche Zugriffsrechte ihnen von den verschiedenen AnbieterInnen von Anwendungen gewährt werden.
- Weil die BenutzerInnen immer mehr Fotos und andere Dateien auf ihren Smartphones speichern und deshalb die Speicherkapazitäten bald erschöpft sein werden.

Übung MULTIPLE CHOICE

Situation: Welche Sicherheitsrisiken und unerwünschten Folgen können Instant-Messaging-Dienste und andere Anwendungen verursachen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Messenger laufen Gefahr, Phishing-Links zu versenden oder Malware über anklickbare Hyperlinks oder übertragene Dateien zu übertragen.
- Malware kann vor allem in kostenlosen Apps von weniger bekannten App-AnbieterInnen vorhanden sein.
- Ein großes Problem sind eher hohe versteckte Kosten als der geheime Zugriff auf persönliche Daten.
- Unverschlüsselte Kommunikation, wie sie z.B. über WhatsApp üblich ist, stellt ein großes Sicherheitsproblem dar.

- Durch verschlüsselte Kommunikation können persönliche Daten verloren gehen.

4. Wissen aufbauen - Maßnahmen und Tipps für die sichere Nutzung von Smartphone-Anwendungen

Angesichts der potenziellen Sicherheitsrisiken bei der Verwendung von Apps auf Ihrem Smartphone fragen Sie sich wahrscheinlich, wie Sie sich und Ihre Privatsphäre besser schützen können. Im Folgenden finden Sie einige Tipps, **was Sie bei der Verwendung von Apps auf Ihrem Smartphone beachten sollten**:

In der Vergangenheit wurden bei verschiedenen Apps gravierende Sicherheitsmängel festgestellt. In der Folge wurde versucht, diese Mängel durch entsprechende Anpassungen zu beheben. Aus diesem Grund ist es zum Beispiel ratsam, immer die **neueste Version des WhatsApp Messengers** zu verwenden.

Um Urheberrechtsprobleme zu vermeiden, sollten **Sie darauf verzichten, Bilder, die Sie nicht besitzen, als Profilbilder zu verwenden.**

Tipp
Sie können auch die Privatsphäre-Einstellungen von WhatsApp verwenden, um **die Sichtbarkeit Ihres Profilbildes einzuschränken**: Öffnen Sie einfach WhatsApp und tippen Sie auf "Einstellungen". Tippen Sie dann auf Konto", wählen Sie Privatsphäre" und ändern Sie die Einstellung Jeder" in Meine Kontakte" oder Niemand" für das Profilbild.

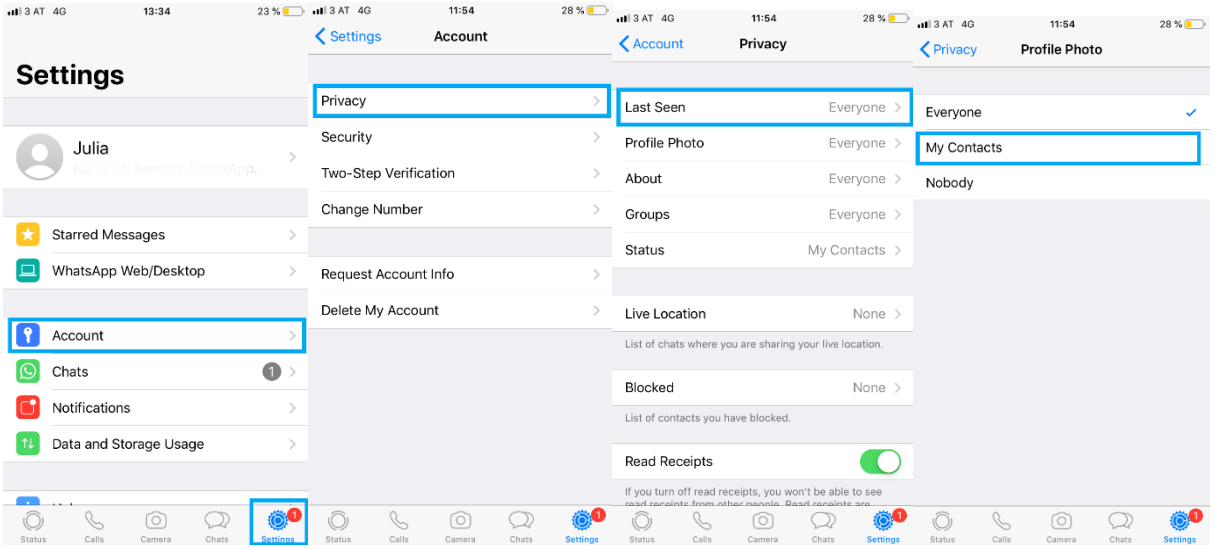
App-AnbieterInnen sind verpflichtet, dem Nutzer bzw. der Nutzerin eine **Datenschutzerklärung** zur Verfügung zu stellen, die Informationen über die von der App beantragten Berechtigungen enthält. Darüber hinaus müssen Sie diesen Berechtigungen bei der Installation der meisten Apps **zustimmen**. Sie sollten die **Datenschutzerklärung** und die Nutzungsbedingungen jeder App vor der Installation **kritisch lesen**. Sie sollten auch die **Zugriffsrechte von Apps kontrollieren**! Die gewährten Berechtigungen können jederzeit in den Einstellungen für jede Anwendung eingesehen und widerrufen werden.

Beispiel
Es ist leicht zu verstehen, dass z.B. eine Wetter-App zur Anzeige der Wettervorhersage in der Lage sein muss, Ihren Standort abzufragen, um genauere Vorhersageinformationen zu erhalten. Warum diese App möglicherweise Zugriff auf die Kamera Ihres Smartphones benötigt, ist jedoch nicht mehr so offensichtlich.

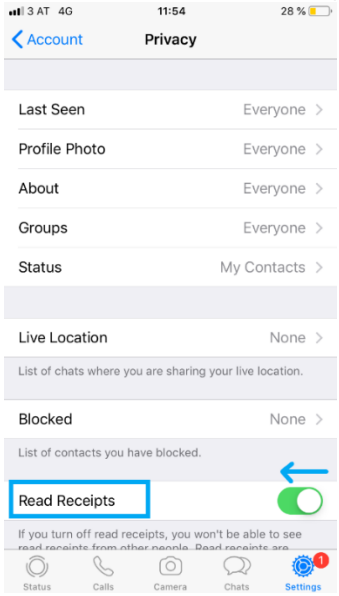
Sie sollten nur die notwendigsten Daten eingeben. Benutzen Sie eine zusätzliche **E-Mail-Adresse**, die nicht viel über Sie verrät und Sie nicht in Sachen Spam belästigt.

Ein angeblich großer Vorteil von IM ist, dass immer sofort ersichtlich ist, wann ein Kontakt online ist oder wann er zuletzt online war. Die neuen Privatsphäre-Einstellungen einiger Messenger bieten Ihnen jedoch die Möglichkeit, **andere davon abzuhalten, zu wissen, dass Sie online sind, wann Sie zuletzt online waren oder automatische Lesebestätigungen abzuschalten**. Wie dies funktioniert, wird im Folgenden am Beispiel von WhatsApp gezeigt:

- **Wie Sie "Zuletzt gesehen" ausblenden**: Öffnen Sie WhatsApp und tippen Sie auf "Konto". Tippen Sie dann auf "Datenschutz", wählen Sie "Zuletzt gesehen" und wählen Sie aus, wer oder ob jemand sehen kann, wann Sie zuletzt online waren.

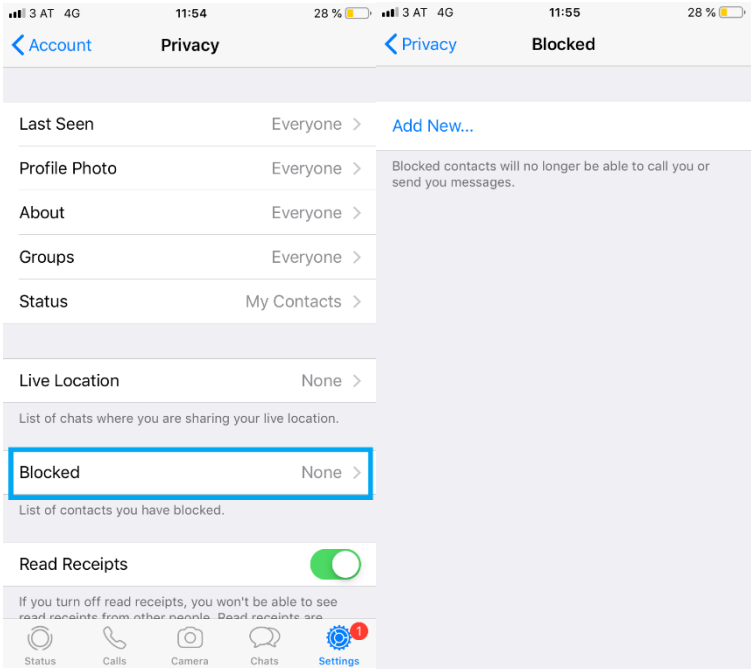


- Wie man Lesebestätigungen ausschaltet: Tippen Sie erneut auf "Einstellungen", "Konto" und "Datenschutz". Dann deaktivieren Sie einfach die Lesebestätigung.



Um den Kontakt durch Fremde zu vermeiden, sollte man sich in erster Linie **immer genau überlegen, in welchen Fällen die Handynummer angegeben** werden sollte und vor allem, wem sie mitgeteilt werden sollte! Wenn unerwünschte Personen versuchen, Sie über WhatsApp zu kontaktieren, können Sie diese einfach blockieren. Scrollen Sie dazu unter "Datenschutz" nach unten und tippen Sie auf blockierte Kontakte.

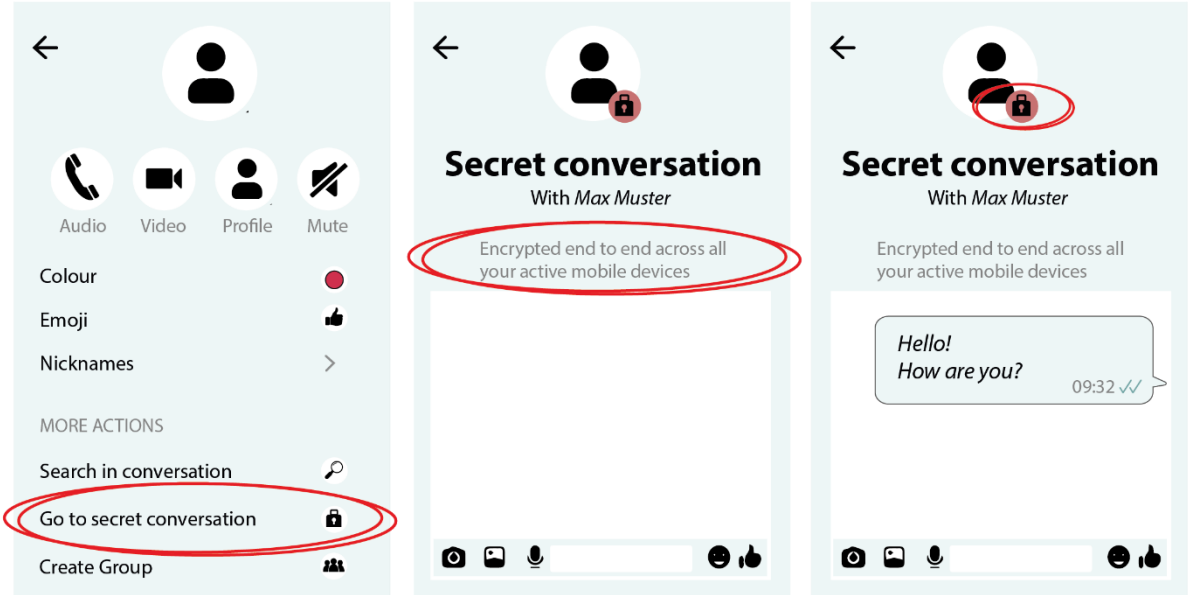
Co-funded by the
Erasmus+ Programme
of the European Union



Wichtig
Blockieren Sie Kontakte, wenn Sie sich nicht sicher sind, wer sie sind oder wenn Sie von jemandem belästigt werden. Melden Sie Beleidigungen, sexuelle Belästigung, Erpressung oder Drohungen bei der Polizei.

Einige Messenger-Anwendungen, wie z. B. Facebook Messenger, **verschlüsseln Ihre Nachrichten nicht automatisch**. Sie sollten die Einstellungen nach Möglichkeit manuell ändern.

So kommunizieren Sie verschlüsselt mit Facebook Messenger: Gehen Sie in den Chat, tippen Sie auf den Namen der Person und wählen Sie "Geheime Konversation". Nun ist der Nachrichtenaustausch mit dieser Person durchgehend verschlüsselt. Niemand außer Ihnen und Ihrem Chat-Partner wird Ihre Nachrichten sehen, auch nicht Facebook.



Tipp

Sie können einen verschlüsselten Chat daran erkennen, dass die Benutzeroberfläche **grau-schwarz** ist. Außerdem sehen Sie auf dem Profilbild Ihres Chatpartners ein **kleines schwarzes Schloss**.

4.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist bei der Nutzung von Apps auf Smartphones zu beachten, um sich und Ihre Privatsphäre zu schützen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Sie sollten die Datenschutzrichtlinie und die Nutzungsbedingungen jeder App kritisch lesen, bevor Sie sie installieren.
- Sie sollten nach Möglichkeit keiner Aktualisierung von Apps zustimmen.
- Es ist nicht sicher, Profilbilder von Ihnen zu verwenden. Es ist besser, Bilder zu verwenden, die Sie nicht selbst aufgenommen, sondern irgendwo im Internet gefunden haben.
- Sie sollten die Zugriffsrechte der Apps kontrollieren und entsprechend anpassen.
- Sie sollten für die Registrierung eine seriöse E-Mail-Adresse verwenden (z.B. bestehend aus Ihrem echten Vor- und Nachnamen).
- Sie sollten nur so viele Angaben zu Ihrer Person machen, wie unbedingt nötig.

Übung MULTIPLE CHOICE

Situation: Was können Sie in Bezug auf Datenschutzeinstellungen in beliebten Anwendungen wie WhatsApp oder Facebook Messenger tun, um Ihre Privatsphäre zu verbessern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Wenn ich beispielsweise WhatsApp verwende, kann ich unter Einstellungen und Datenschutz deaktivieren, dass andere Benutzer sehen können, wann ich zuletzt online war.
- So kann ich beispielsweise unter Einstellungen und Datenschutz den Zugriff von WhatsApp auf meine Kontakte unter Einstellungen und Datenschutz deaktivieren.
- Wenn ich WhatsApp verwende, kann ich unter Einstellungen, Account und Datenschutz auch die Lesebestätigung deaktivieren oder unerwünschte Kontakte blockieren.
- Ich kann auch den Facebook Messenger verwenden, um verschlüsselt mit meinen Freunden zu kommunizieren: Dazu gehe ich in den jeweiligen Chat, wähle den Namen der Person aus und starte einfach ein geheimes Gespräch.
- Um mit Kontakten zu kommunizieren, die auf WhatsApp blockiert sind, wähle ich den Namen der Person aus und starte eine "geheime Konversation".

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

Quellen

klicksafe.de: https://www.klicksafe.de/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/was-ist-der-whatsapp-messenger/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/probleme-mit-dem-whatsapp-messenger/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/whatsapp/schritt-fuer-schritt/kontakte-blockieren/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/faq/was-ist-eine-geheime-unterhaltung-im-messenger/

saferinternet.at:https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/schritt-fuer-schritt/verschluesselt-chatten/

digitaltrends.com: https://www.digitaltrends.com/mobile/how-to-protect-your-smartphone-from-hackers-and-intruders/

techsafe.org: https://www.techsafety.org/12tipscellphones

avast.com: https://blog.avast.com/9-smartphone-tips-privacy-security

fraud-magazine.com: https://www.fraud-magazine.com/article.aspx?id=4294992799

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

Wissen sichern

Zusammenfassung

Für die meisten von uns ist ihr **Smartphone** ein integraler Bestandteil des täglichen Lebens. Deshalb sollten wir nicht vergessen, die privaten Informationen und Daten, die darauf gespeichert sind, entsprechend zu schützen. So ist es beispielsweise bei Verlust oder Diebstahl Ihres Smartphones sinnvoll, eine **sichere PIN** (nicht eine Zahlenkombination wie 1234) und ein **Bildschirmschloss** zu verwenden. Sie sollten auch in Erwägung ziehen, eine Art **Anti-Diebstahl-App** zu installieren.

Instant-Messaging-Anbieter wie **WhatsApp** erfreuen sich immer größerer Beliebtheit. Wenn Sie diese oder andere Anwendungen verwenden, sollten Sie jedoch immer überlegen, **welche Zugriffsrechte Sie der Anwendung gewähren**, und diese auf ein Minimum beschränken.

Haben Sie sich schon einmal gefragt, warum die Nutzung von WhatsApp kostenlos ist? Wenn Sie kostenlose Apps verwenden, sollten Sie sich dessen immer bewusst sein: Wenn Sie für das Produkt nicht bezahlen müssen, sind **in der Regel Sie oder Ihre Daten das Produkt**. Darüber hinaus besteht die Gefahr, dass in Anwendungen **verschiedene Malware** versteckt ist, insbesondere wenn diese Anwendungen kostenlos im Internet und von wenig bekannten AnwendungsanbieterInnen vertrieben werden. Ein weiteres Sicherheitsrisiko ist die Tatsache, dass einige Anbieter von Online-Kommunikation **die Kommunikation nicht verschlüsseln** (z.B. Facebook Messenger).

Durch die Übernahme von WhatsApp durch Facebook sind viele NutzerInnen kritischer geworden, was die Datenschutzrichtlinien dieser Dienste betrifft. Die Anwendungen werden daher ständig hinsichtlich ihrer Datenschutzbestimmungen optimiert. Aus diesem Grund ist es z.B. sinnvoll, immer die **neueste Version des WhatsApp Messengers** zu nutzen. Darüber hinaus sollten Sie vor der Verwendung von Apps **die Datenschutzbestimmungen der von Ihnen verwendeten App lesen**, die Zugriffsrechte der App überprüfen und gegebenenfalls anpassen. Sie können auch die **Datenschutzeinstellungen von Apps leicht anpassen**, z. B. die Sichtbarkeit des Profilbildes auf WhatsApp oder das Blockieren unerwünschter Kontakte.

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

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche Maßnahmen können Sie ergreifen, um Ihr Smartphone vor unberechtigtem Zugriff zu schützen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Ich kann eine PIN verwenden. Diese PIN sollte so einfach wie möglich zu merken sein.
- **Ich sollte mein Smartphone mit einer PIN sperren und sicherstellen, dass es sich nicht um eine Zahlenkombination wie 1234 oder 1111 handelt.**
- **Ich kann eine Bildschirmsperre einrichten.**
- Ich kann eine kostenpflichtige Anwendung installieren, um eine persönliche Identifikationsnummer einzurichten.

Übung MULTIPLE CHOICE

Situation: Nach einem Einkaufsnachmittag in der Stadt stellen Sie zu Hause plötzlich fest, dass Sie Ihr Smartphone verloren haben. Welche Maßnahmen können in einer solchen Situation sinnvoll sein?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Ich kann den Android Device Manager oder die iCloud verwenden, um mein Smartphone zu lokalisieren.**
- **Ich kann eine Art Anti-Diebstahl-App für solche Fälle installieren. Damit kann ich mein Telefon lokalisieren, sperren oder gespeicherte Daten auf dem Telefon löschen.**
- Ich kann meine SIM-Karte sperren lassen, damit ich mein Telefon lokalisieren kann.
- **Ich kann meine SIM-Karte sperren lassen, um zu verhindern, dass jemand durch die Benutzung meines Telefons hohe Kosten verursacht.**

2.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen über Instant Messaging (IM)-Dienste sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- **Immer mehr Menschen nutzen IM-Dienste zum Austausch von Textnachrichten, während die Kommunikation per SMS an Beliebtheit verloren hat.**
- **IM ist Internet-basierte Kommunikation.**
- **IM ermöglicht nicht nur den Austausch von Textnachrichten, sondern auch den Austausch von Dateien, Audios oder die Kommunikation über Video-Chat.**
- Wenn viele Menschen gleichzeitig beliebte IM-Dienste nutzen, dauert es in der Regel einige Minuten, bis der Empfänger die Nachrichten erhält.
- **Beliebte IM-Dienste sind Facebook Messenger, WhatsApp oder Windows Life Messenger.**

- Beliebte IM-Dienste sind Youtube, Twitter, WhatsApp und Google.

Übung MULTIPLE CHOICE

Situation: Sie möchten WhatsApp verwenden, um mit Ihren Freunden zu kommunizieren. Was sollten Sie bei der Installation der App beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Messenger-Apps wie WhatsApp erfordern in der Regel die einmalige Zahlung einer Nutzungsgebühr im Voraus.
- Um WhatsApp nutzen zu können, müssen Sie die Anwendung herunterladen und sich mit Ihrem echten Namen registrieren.
- **WhatsApp greift auf alle in Ihrem Smartphone gespeicherten Kontakte zu.**
- **Um bestimmte Dienste von WhatsApp nutzen zu können, kann es erforderlich sein, der App den Zugriff auf Ihre Bilder, Kamera, Mikrofon oder Standortdaten zu erlauben.**
- WhatsApp greift automatisch auf alle in Ihrem Smartphone gespeicherten Kontakte, Ihre Bilder und Ihre Standortdaten zu. Dies ist die einzige Möglichkeit, wie die App funktionieren kann.

Übung MULTIPLE CHOICE

Situation: Wann ist es sinnvoll, App-Berechtigungen anzupassen und wie ist dies grundsätzlich möglich?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Grundsätzlich können Sie unter "Einstellungen" leicht überprüfen, welche der installierten Apps welche Zugriffsrechte besitzen und diese ggf. auf das wirklich notwendige Maß reduzieren.**
- Um herauszufinden, welche Zugriffsrechte eine App hat, ist es ratsam, Ihren Mobilfunkanbieter anzurufen.
- **Wenn Sie z.B. Google Maps verwenden möchten, ist es sinnvoll, der App den Zugriff auf Ihre Standortdaten zu erlauben, während Sie die App benutzen.**
- Es ist auch eine gute Idee, WhatsApp den Zugriff auf Ihre Standortdaten zu gestatten, da dies dazu beiträgt, dass Ihre Nachrichten schneller übertragen werden.
- Da die meisten Apps kostenlos sind, ist es in der Regel nicht möglich, die Zugriffsrechte der Apps einzeln einzuschränken.

3.Wissen anwenden

Übung SINGLE CHOICE

Situation: Warum sind die NutzerInnen von Apps zunehmend besorgt über den Datenschutz?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Weil Apps von immer mehr Menschen genutzt werden
- Weil die Apps in erster Linie von Unternehmen entwickelt werden, die in Ländern ansässig sind, die sich nicht um den Datenschutz kümmern, und es daher keine verbindlichen Datenschutzregeln für den Umgang mit Benutzerdaten gibt. Ein bekanntes Beispiel ist Facebook oder WhatsApp.
- Weil die Apps immer teurer werden.
- **Weil in den letzten Jahren einige Datenschutzverletzungen bekannt geworden sind.**

- Weil es für BenutzerInnen nicht nachvollziehbar ist, welche Zugriffsrechte ihnen von den verschiedenen AnbieterInnen von Anwendungen gewährt werden.
- Weil die BenutzerInnen immer mehr Fotos und andere Dateien auf ihren Smartphones speichern und deshalb die Speicherkapazitäten bald erschöpft sein werden.

Übung MULTIPLE CHOICE

Situation: Welche Sicherheitsrisiken und unerwünschten Folgen können Instant-Messaging-Dienste und andere Anwendungen verursachen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Messenger laufen Gefahr, Phishing-Links zu versenden oder Malware über anklickbare Hyperlinks oder übertragene Dateien zu übertragen.**
- **Malware kann vor allem in kostenlosen Apps von weniger bekannten App-AnbieterInnen vorhanden sein.**
- Ein großes Problem sind eher hohe versteckte Kosten als der geheime Zugriff auf persönliche Daten.
- Unverschlüsselte Kommunikation, wie sie z.B. über WhatsApp üblich ist, stellt ein großes Sicherheitsproblem dar.
- Durch verschlüsselte Kommunikation können persönliche Daten verloren gehen.

4.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist bei der Nutzung von Apps auf Smartphones zu beachten, um sich und Ihre Privatsphäre zu schützen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Sie sollten die Datenschutzrichtlinie und die Nutzungsbedingungen jeder App kritisch lesen, bevor Sie sie installieren.**
- Sie sollten nach Möglichkeit keiner Aktualisierung von Apps zustimmen.
- Es ist nicht sicher, Profilbilder von Ihnen zu verwenden. Es ist besser, Bilder zu verwenden, die Sie nicht selbst aufgenommen, sondern irgendwo im Internet gefunden haben.
- **Sie sollten die Zugriffsrechte der Apps kontrollieren und entsprechend anpassen.**
- Sie sollten für die Registrierung eine seriöse E-Mail-Adresse verwenden (z.B. bestehend aus Ihrem echten Vor- und Nachnamen).
- **Sie sollten nur so viele Angaben zu Ihrer Person machen, wie unbedingt nötig.**

Übung MULTIPLE CHOICE

Situation: Was können Sie in Bezug auf Datenschutzeinstellungen in beliebten Anwendungen wie WhatsApp oder Facebook Messenger tun, um Ihre Privatsphäre zu verbessern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Wenn ich beispielsweise WhatsApp verwende, kann ich unter Einstellungen und Datenschutz deaktivieren, dass andere Benutzer sehen können, wann ich zuletzt online war.**

- So kann ich beispielsweise unter Einstellungen und Datenschutz den Zugriff von WhatsApp auf meine Kontakte unter Einstellungen und Datenschutz deaktivieren.
- Wenn ich WhatsApp verwende, kann ich unter Einstellungen, Account und Datenschutz auch die Lesebestätigung deaktivieren oder unerwünschte Kontakte blockieren.
- Ich kann auch den Facebook Messenger verwenden, um verschlüsselt mit meinen Freunden zu kommunizieren: Dazu gehe ich in den jeweiligen Chat, wähle den Namen der Person aus und starte einfach ein geheimes Gespräch.
- Um mit Kontakten zu kommunizieren, die auf WhatsApp blockiert sind, wähle ich den Namen der Person aus und starte eine "geheime Konversation"