Módulo de aprendizagem

Proteção de *Smartphones*

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do autor: bit schulungscenter
Última data de processamento: 28.10.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Proteção de *Smartphone*

Introdução

Redes sociais, mensagens instantâneas, compras, jogos, aplicações, tirar uma foto rápida ou fazer algumas pesquisas no Google - muitas pessoas dificilmente conseguem imaginar a vida quotidiana sem o seu *smartphone*. No entanto, para fazer telefonemas, é usado cada vez menos. A tendência clara é digitar em vez de fazer telefonemas. Isto também é se nota quando vemos o número de utilizadores de serviços de mensagens instantâneas: cerca de 1,6 mil milhões de pessoas em todo o mundo usam o WhatsApp, e cerca de 1,3 mil milhões comunicam com os amigos através do Facebook Messenger. Usar estes serviços é uma brincadeira de crianças. Mas quais os perigos que estão à espreita quando se usam serviços de mensagens instantâneas ou outras aplicações de *smartphones* no que diz respeito à privacidade dos dados? Não é à toa que o Facebook e outros fornecedores de aplicativos gratuitos de *smartphones* são repetidamente criticados pelos protecionistas de dados. Descobre como podes proteger melhor o teu *smartphone*, os teus dados e a tua privacidade!

Relevância Prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

Depois de completar esta unidade de conteúdo, serás capaz de avaliar melhor os riscos associados ao uso de serviços de mensagens instantâneas ou outras aplicações de *smartphone*, e ficarás a conhecer alguns passos úteis para proteger o teu telefone e a tua privacidade de riscos indesejados.

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

1.Desenvolver conhecimento – Medidas básicas de proteção dos *smartphones*

Para muitas pessoas, o *smartphone* é um companheiro constante na vida quotidiana. Também fazes parte do grupo de pessoas que levam o seu *smartphone* para todo o lado e não conseguem passar um dia sem ele? Se sim, provavelmente também tens dados **muito privados ou sensíveis no teu *smartphone***, como fotos, mensagens de texto confidenciais ou informações de negócio. A fim de proteger o telemóvel e os dados potencialmente muito privados que armazenas, deverás tomar as medidas adequadas em caso de perda ou roubo.

Isto inclui, por exemplo, a proteção do *smartphone* contra acessos não autorizados via **PIN** (Número de Identificação Pessoal, ou *Personal Identification Number*, em inglês) e o **bloqueio do ecrã**.

Importante
Certifica-te de que **não utilizas combinações de números comuns** tais como "1234", "1111" ou outras similares. É muito fácil para pessoas não autorizadas *hackearem* essas combinações.

Na eventualidade de um *smartphone* ser roubado ou perdido, deve-se sempre proceder ao bloqueamento do **cartão SIM** (módulo de identidade do subscritor) do dispositivo **bloqueado** pelo respetivo fornecedor de rede, para que ninguém o possa utilizar para fazer chamadas telefónicas ou incorrer em custos elevados.

Sabes o **número de série do teu *smartphone***? Este está localizado debaixo da bateria, na embalagem original, ou na fatura de compra do telemóvel. Deves tomar nota deste número para que o possas denunciar à polícia em caso de roubo.

Todos os sistemas operativos comuns também oferecem **vários serviços** que podem ser muito úteis em caso de roubo ou perda.

Exemplos
Não consegues encontrar o telemóvel? Com o **Android Device Manager** é possível pôr o *smartphone* a tocar no volume máximo, mesmo que este tenha sido silenciado. Desta forma, consegue-se localizar rapidamente um telemóvel perdido em casa. Se estiver noutro sítio, a plataforma permite localizá-lo em tempo real e deixar uma mensagem para quem encontrar o telemóvel. Se um iPhone tiver sido perdido ou roubado, normalmente é possível procurá-lo através do **iCloud**, desde que o aparelho esteja ligado e tenha receção de dados.

Provavelmente já ouviste falar da possibilidade de instalar uma espécie de **aplicação antirroubo** no *smartphone*. Esta permite, por exemplo, localizar e bloquear o *smartphone* perdido ou roubado e apagar os dados armazenados no mesmo. Os comandos necessários para tal podem ser emitidos por outro *smartphone* cujo número tenha sido armazenado ou enviado para o dispositivo através de um portal *online*.

Dica
Em caso de roubo ou perda, deves bloquear imediatamente o cartão SIM **se não tiveres uma aplicação antirroubo instalada no teu telefone**. No entanto, se estiver instalada uma aplicação semelhante, o cartão SIM não deve ser bloqueado até que os dados tenham sido localizados e remotamente apagados. Caso contrário, isto deixa de ser possível.

1.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_01_01

Situação: Que medidas podem ser tomadas para proteger o *smartphone* de acessos não autorizados?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Usar um PIN que seja o mais fácil de memorizar possível.
- Bloquear o *smartphone* com um PIN, garantindo que não é uma combinação de números como 1234 ou 1111.
- Configurar um bloqueio de ecrã.
- Instalar uma aplicação paga para estabelecer um número de identificação pessoal (PIN).

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_01_02

Situação: Quando chegas a casa de uma tarde de compras na cidade, apercebes-te subitamente que perdeste o *smartphone*. Que medidas podem ser úteis numa situação destas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Usar o Android Device Manager ou o iCloud para localizar o *smartphone.*
- Instalar algum tipo de aplicação anti-roubo para este tipo de situações. Isto permite localizar o telefone, bloqueá-lo ou apagar os dados armazenados no *smartphone*.
- Bloquear o cartão SIM para localizar o telemóvel posteriormente.
- Bloquear o cartão SIM para evitar que alguém incorra em custos elevados ao usar o telemóvel perdido.

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

2.Desenvolver conhecimento – Mensagens Instantâneas e Aplicações

A possibilidade de troca de mensagens de texto através do telemóvel não é nova. No entanto, nos últimos anos, devido à utilização generalizada de *smartphones*, a comunicação via SMS tem sido cada vez mais substituída pela utilização de serviços de **mensagens instantâneas** (**IM** – *instant messaging*, em inglês).

Definição
Em contraste com as SMS, as **mensagens instantâneas** são um tipo de **comunicação baseada na Internet** através de **aplicações móveis**. É um tipo de *chat online* que lhe permite trocar mensagens com outros utilizadores em tempo quase real. Para tal, as aplicações de mensagens instantâneas devem ser descarregadas e instaladas.

Para além da transmissão de mensagens, o envio de ficheiros, áudios e vídeo (e, portanto, também videochamadas) normalmente também é possível. O envio de mensagens recorre ao chamado procedimento "*push*", que permite que os destinatários recebam as mensagens imediatamente após terem sido enviadas. Ao contrário dos *emails*, por exemplo, as mensagens não têm de ser recuperadas primeiro, mas aparecem imediatamente no ecrã do parceiro de comunicação.

Exemplo:
Exemplos de serviços de mensagens instantâneas populares: • *Windows life messenger* • *Skype* • *Facebook Messenger* • *WhatsApp* • *WeChat* • *Telegram*

Por exemplo, cerca de 1,3 mil milhões de utilizadores em todo o mundo já utilizam o Facebook Messenger para comunicar.

O uso mais comum de programas de mensagens instantâneas é em dispositivos móveis, tais como ***smartphones*** através de aplicações para o efeito. Estas são geralmente gratuitas, práticas, fáceis de usar e, por isso, gozam de uma popularidade crescente. Para utilizar o WhatsApp, por exemplo, só é necessário descarregar a aplicação gratuita e fazer um registo através do próprio número de telemóvel.

Contudo, para cumprir o objetivo desejado, uma aplicação normalmente requer uma variedade de autorizações. Portanto, a aplicação pretende aceder a determinadas funções do seu *smartphone*, tais como o calendário, câmara, contactos, microfone, SMS, memória, localização ou especificidades funcionais do telefone.

Importante
És uma das 1,6 mil milhões de pessoas que usam o WhatsApp em todo o mundo? Então deves estar ciente de que o WhatsApp acede a (pelo menos) **todos os contactos armazenados no teu telemóvel**.

Essa é a única maneira da aplicação determinar quais dos teus contactos também usam o WhatsApp, de maneira a exibi-los automaticamente na aplicação. Queres enviar fotografias ou a tua localização

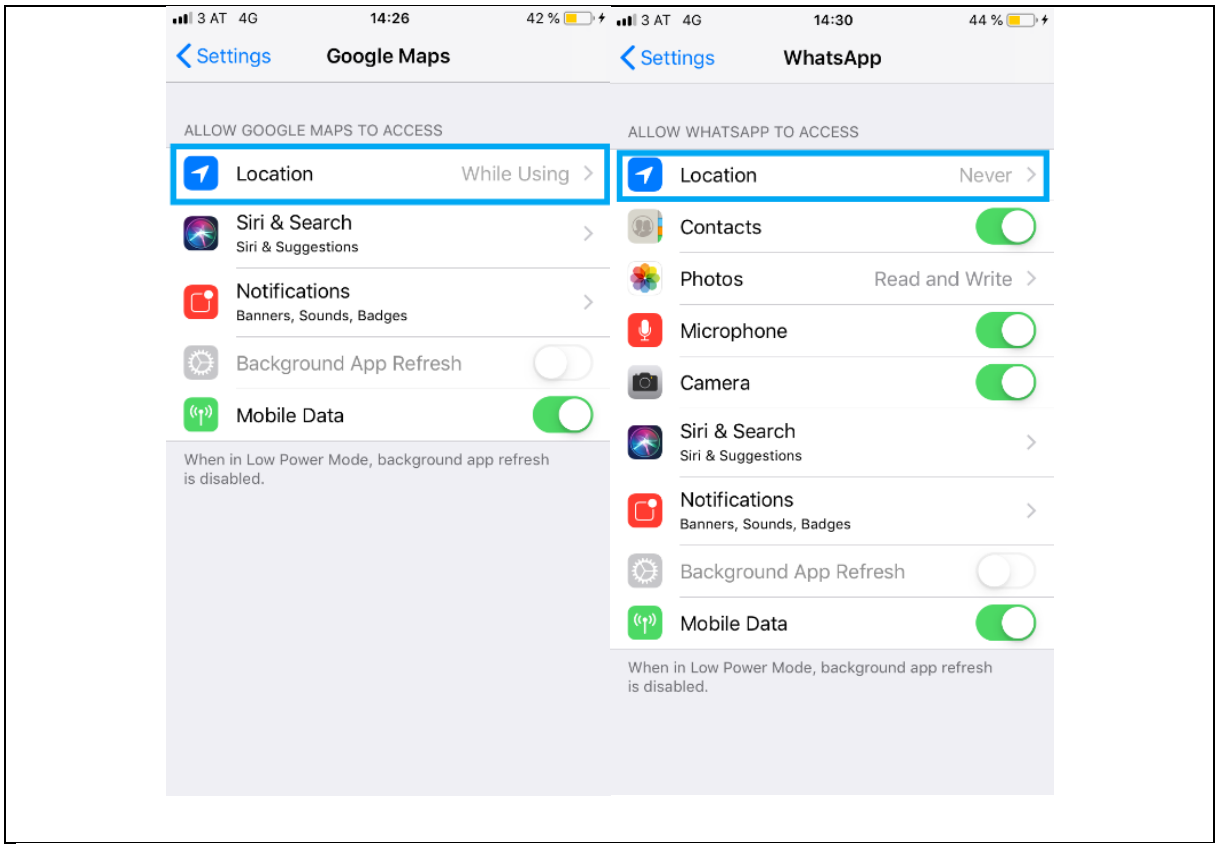
através do WhatsApp ou utilizar a aplicação para fazer videochamadas? Se sim, lembra-te que o WhatsApp também precisa de aceder às tuas fotografias, câmara, microfone e dados de localização!

Dica
Devido a razões de proteção de dados, vale a pena ter cuidado ao atribuir **autorizações às aplicações** e reduzir as autorizações ao nível mínimo, atribuindo apenas as mais necessárias.

Se não tiveres a certeza sobre quais as permissões que cada aplicação tem no teu *smartphone*, deves verificar isto, por razões de segurança. Para fazê-lo, basta selecionar a aplicação em questão nas Definições, ver quais os acessos permitidos à aplicação e ajustá-los se necessário.

Exemplo
Imagina que queres usar o Google Maps para encontrar uma morada específica. Neste caso, faz sentido permitir que essa *app* **aceda à tua localização enquanto a usas**. Contudo, se não quiseres partilhar a tua localização com os teus contactos do WhatsApp, a aplicação não precisa necessariamente de saber onde estás.

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



2.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_01

Situação: Quais das seguintes afirmações sobre mensagens instantâneas são verdadeiras?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.Cada vez mais pessoas utilizam os serviços de mensagens instantâneas para trocar mensagens de texto, enquanto que a comunicação via SMS tem perdido popularidade.

- As mensagens instantâneas são comunicações baseadas na Internet.
- As mensagens instantâneas permitem não só a troca de mensagens de texto, mas também a troca de ficheiros, áudios ou videochamadas.
- Se muitas pessoas utilizarem os mesmos serviços de mensagens instantâneas ao mesmo tempo, normalmente demora alguns minutos até que o destinatário receba as mensagens.
- Os serviços mais populares de mensagens instantâneas são o Facebook Messenger, o WhatsApp ou o Windows life messenger.
- Os serviços mais populares de mensagens instantâneas são o Youtube, Twitter, WhatsApp e Google.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_02

Situação: Queres usar o WhatsApp para comunicar com os teus amigos. O que deves ter em mente quando instalas a aplicação?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Aplicações como o WhatsApp requerem normalmente o pagamento de uma taxa única de utilização com antecedência.
- Para usar o WhatsApp, é necessário descarregar a aplicação e fazer um registo com o nome verdadeiro.
- O WhatsApp acede a todos os contactos armazenados no *smartphone*.
- Para utilizar determinados serviços do WhatsApp, pode ser necessário permitir que a aplicação aceda às imagens, câmara, microfone ou dados de localização do telemóvel.
- O WhatsApp acede automaticamente a todos os contactos armazenados no *smartphone*, às fotografias e aos dados de localização. Se não tiver acesso a estes dados, a aplicação não funciona.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_03

Situação: Quando é que faz sentido ajustar as autorizações das aplicações e como é que é possível fazê-lo?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Basicamente, é possível verificar nas "Definições" quais das aplicações instaladas têm direitos de acesso e, se necessário, reduzir os acessos ao mínimo necessário.
- Para perceber quais os direitos de acesso que uma aplicação tem é necessário contactar a tua operadora.
- Se queres usar o Google Maps, por exemplo, deves permitir que a aplicação aceda aos dados da localização durante o uso.
- Também é boa ideia permitir que o WhatsApp aceda aos dados de localização, uma vez que isso permite uma mais rápida transferência de mensagens.
- Uma vez que a maioria das aplicações não acarreta custos, normalmente não é possível restringir os direitos de acesso de cada uma das aplicações.

3.Desenvolver conhecimento – Riscos de segurança no uso de aplicações para *smartphone*

Se também tendes a armazenar e processar muitos dados no teu *smartphone*, particularmente dados de natureza muito privada e de terceiros (por exemplo, fotos), deves repensar até que ponto é que as **permissões ilimitadas das aplicações** podem ser problemáticas.

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

Não é segredo que muitos criadores de aplicações estão interessados na tua informação pessoal. Afinal de contas, eles precisam de gerar algum tipo de lucro com as aplicações que são, normalmente, providenciadas gratuitamente aos utilizadores. Costuma-se dizer que **se não estás a pagar pelo produto então, normalmente, és tu o produto.**

No entanto, **a aquisição do WhatsApp pelo Facebook**, por exemplo, significa que os números de telefone da lista de contactos são obtidos não só pelo WhatsApp mas, por intermédio desse, também pelo Facebook. Além disso, a descoberta de vários incidentes de violação da privacidade em anos recentes também levou a uma maior consciencialização dos perigos da monitorização não autorizada. Os utilizadores estão cada vez mais preocupados com a proteção de dados.

Já estás a questionar-te quais os problemas de segurança e consequências indesejadas que podem surgir da utilização de serviços de mensagens instantâneas e outras aplicações? Seguem alguns exemplos:

- Tal como com outros meios de comunicação *online*, os utilizadores das aplicações de mensagens instantâneas também correm o risco de receber **ligações de *phishing* ou transmitir *malware*** através de hiperligações clicáveis ou ficheiros transferidos.
- Existe o perigo de haja **todo o tipo de *malware* escondido nas aplicações**, especialmente se estas tiverem sido adquiridas gratuitamente na Internet a provedores de aplicações menos fiáveis.
- Como já é do teu conhecimento, as aplicações pedem permissões para executar certas funções. As permissões permitem às aplicações a leitura de dados. Assim, existe o **risco de acesso oculto a dados pessoais**, tais como dados de localização, hábitos de navegação *online*, dados de contacto armazenados ou palavras-passe. Para além da perda de privacidade, a **utilização indevida dos seus dados** também pode ser uma consequência desagradável.
- Podem surgir **problemas com direitos de autor**, por exemplo, usares como foto de perfil imagens que não são da tua autoria e para as quais não possuis os direitos de autor.
- A **comunicação não encriptada** representa um elevado risco de segurança. Portanto, desde Abril de 2016, o conteúdo enviado através do WhatsApp, por exemplo, tem sido transmitido com encriptação segura de ponta a ponta. Isto aplica-se a textos, imagens, vídeos e outros ficheiros. A encriptação de ponta a ponta significa que apenas as pessoas com quem estamos a comunicar podem receber e ler o conteúdo.

Importante
Se utilizares a aplicação Facebook Message, tem em consideração que a tua comunicação (ao

contrário do WhatsApp) não é encriptada! Se quiseres uma comunicação encriptada de ponta a ponta, deves iniciar uma "conversa secreta". A próxima secção explicará como isto funciona.

3.Aplicar conhecimento

Exercício de OPÇÃO ÚNICA

Objetivo específico associado: OE_03_01

Situação: Porque é que os utilizadores de *apps* estão cada vez mais preocupados com a privacidade dos seus dados?
Tarefa: Escolha a opção correta de acordo com o princípio de opção única: apenas uma resposta é verdadeira

- Porque as aplicações são cada vez mais usadas por um número cada vez maior de pessoas.
- Porque as aplicações são primeiramente desenvolvidas por empresas sediadas em países que não se preocupam com a proteção de dados e, por conseguinte, não existem regras vinculativas de proteção de dados para o tratamento de dados dos utilizadores. Um bom exemplo disso é o Facebook ou o WhatsApp.
- Porque as aplicações estão a tornar-se cada vez mais caras.
- Porque alguns casos de violações da proteção de dados se tornaram conhecidos nos últimos anos.
- Porque é impossível aos utilizadores compreender que direitos de acesso concedem aos vários provedores de aplicações.
- Porque os utilizadores estão a armazenar cada vez mais fotografias e outros ficheiros nos seus *smartphones* e, portanto, as capacidades de armazenamento vão esgotar-se em breve.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_03_02

Situação: Quais são os riscos de segurança e consequências indesejadas que podem advir de serviços de mensagens instantâneas e outras aplicações?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- As aplicações de mensagens instantâneas estão ligadas a riscos de *phishing* ou transmissão de *malware* através de hiperligações clicáveis ou ficheiros transferidos.
- O *malware* pode estar presente especialmente em aplicações gratuitas de provedores de aplicações menos conhecidos.
- Os custos ocultos bastante altos são um problema maior do que o acesso secreto a dados pessoais.
- A comunicação não encriptada, como ocorre, por exemplo, no WhatsApp é um grande problema de segurança.
- Os dados pessoais podem ser extraviados durante uma comunicação encriptada.

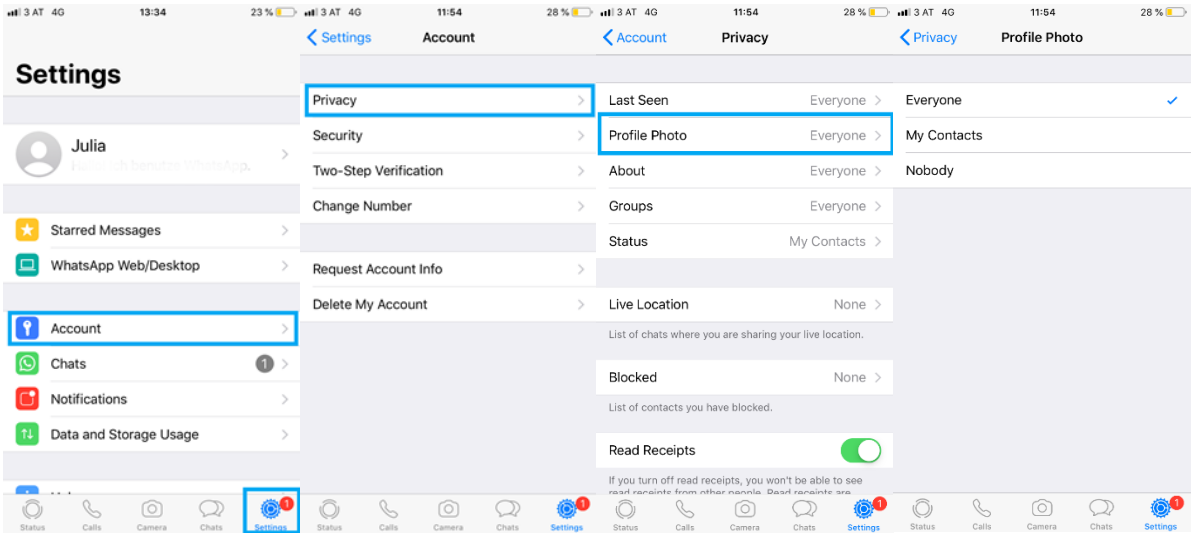
4. Desenvolver conhecimento – Medidas e dicas para o uso seguro de aplicações para *smartphone*

Dados os potenciais riscos de segurança advindos da utilização de *apps* no seu *smartphone*, provavelmente estás a perguntar-te como podes proteger-te melhor e salvaguardar a tua privacidade. Seguem algumas dicas sobre **o que deves considerar quando utilizares aplicações no *smartphone***:

No passado, foram identificadas graves deficiências de segurança em várias aplicações. Subsequentemente, foi feita uma tentativa para remediar estas debilidades, fazendo os ajustamentos adequados. Por este motivo é aconselhável utilizar sempre, por exemplo, a versão mais recente do WhatsApp.

Para evitar problemas de direitos de autor, é importante evitares utilizar imagens que não possuis como imagens de perfil.

Dica
Também podes utilizar as definições de privacidade do WhatsApp para **limitar a visibilidade da tua imagem de perfil**: Basta abrir o WhatsApp e clicar em "Definições". Depois de premir "Conta", seleciona "Privacidade" e altera a definição "Todos" para "Os meus contactos" ou "Ninguém" para limitar a visibilidade da tua foto de perfil.



Os criadores das aplicações são obrigados a fornecer ao utilizador uma **declaração de protecção de dados** que contenha informações sobre as permissões solicitadas pela aplicação. Além disso, a maioria das aplicações hoje em dia **exigem que o utilizador concorde com estas permissões** quando estas são instaladas. É importante **ler sempre a política de privacidade** e os termos e condições de cada aplicação de forma crítica antes da instalação. É também crucial **controlar os direitos de acesso das aplicações**! As permissões concedidas podem ser visualizadas e revogadas em qualquer altura nas definições de cada aplicação.

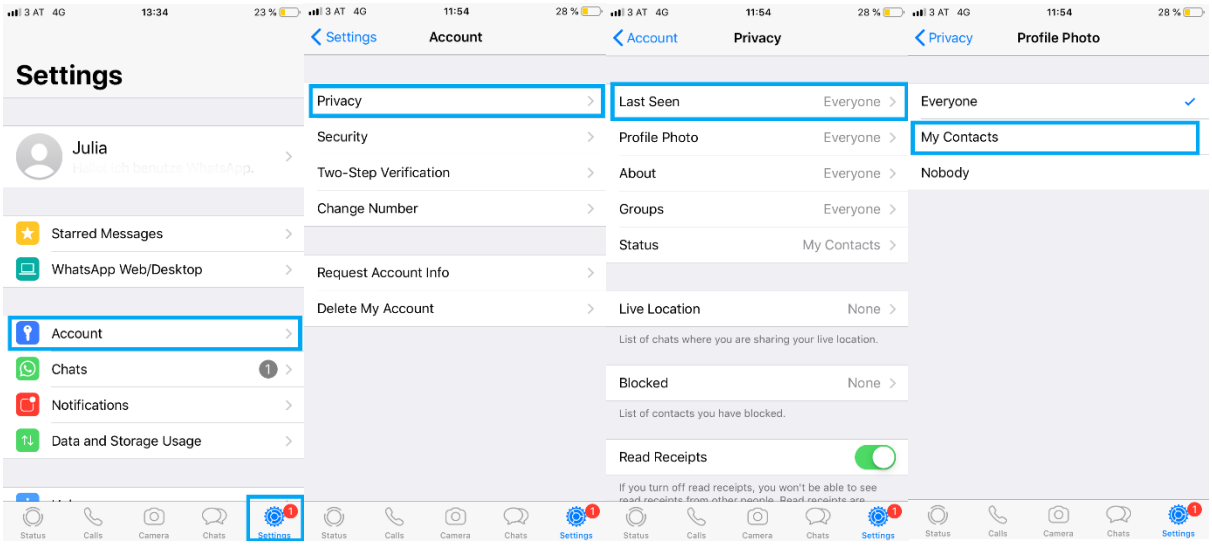
Exemplo
É fácil de compreender que, por exemplo, uma aplicação meteorológica, de modo a exibir a previsão do tempo, deve poder consultar a localização atual para fornecer informações mais precisas. No entanto, a razão pela qual esta aplicação pode precisar de acesso à câmara do *smartphone* já não é tão óbvia.

Deves introduzir apenas os dados estritamente necessários. Usa um **endereço de *email* adicional** que não revele muito sobre ti e que não te incomode com *emails* de *spam*.

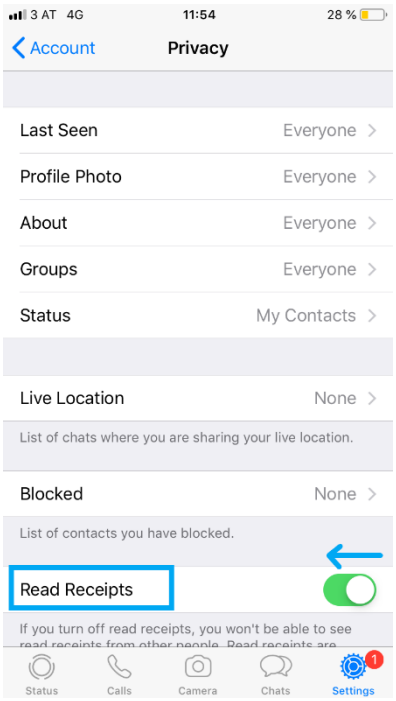
Uma suposta grande vantagem das *apps* de mensagens instantâneas é que é sempre visível quando um contacto está *online* ou quando esteve *online* recentemente. Contudo, novas definições de privacidade de alguns destes serviços oferecem a possibilidade de **impedir que os outros saibam**

quando estamos *online*, quando estivemos *online* pela última vez ou de desligar as confirmações automáticas de leitura. O exemplo seguinte, do WhatsApp, mostra como isto funciona:

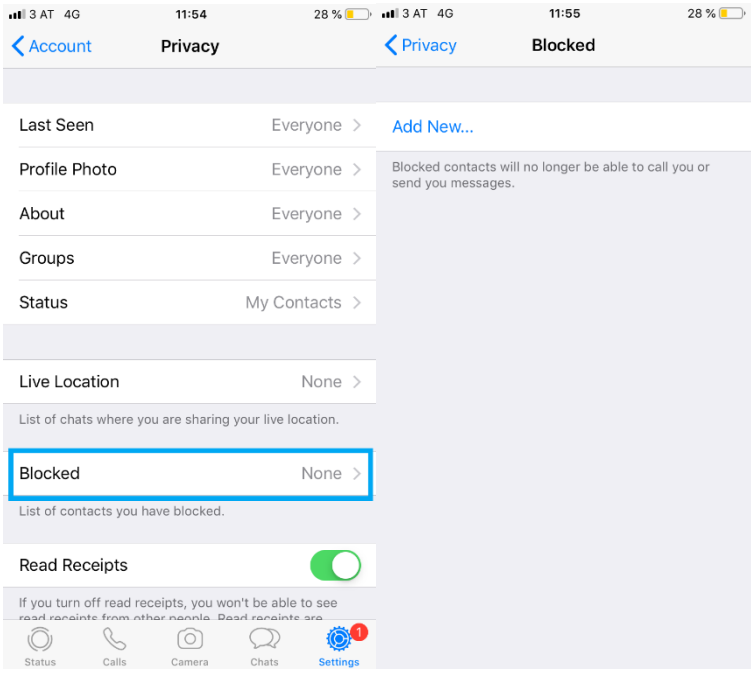
- Como ocultar quando estiveste *online* pela última vez: Abre o WhatsApp e clica em "Definições" e depois "Conta". Depois seleciona "Privacidade", seleciona "Última vez *online*" e escolhe quem ou se alguém pode ver quando estiveste *online* pela última vez.



- Como desligar os recibos de leitura: Clica novamente em "Definições" e "Conta". Depois, seleciona "Privacidade" e desativa os recibos de leitura.



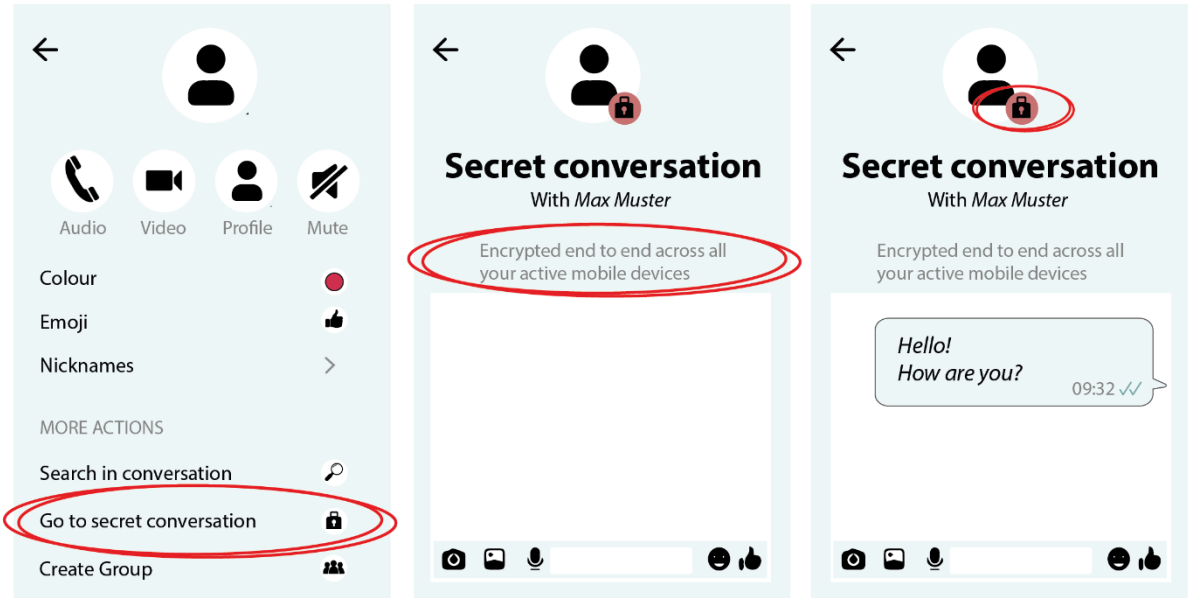
A fim de evitar o contacto por parte de estranhos, em primeiro lugar, deve-se sempre considerar cuidadosamente em que situações se dá o número de telemóvel e, acima de tudo, a quem! Se pessoas indesejadas tentarem contactar-te através do WhatsApp, podes simplesmente bloqueá-los. Para o fazer, entra em "Privacidade" e clica em "Contactos bloqueados".



Importante
Bloqueia contactos se não estiveres seguro de quem são ou se alguém te estiver a assediar. Comunica quaisquer insultos, assédio sexual, chantagem ou ameaças diretamente à polícia.

Algumas aplicações de mensagens instantâneas, como o Facebook Messenger, **não encriptam automaticamente as mensagens**. Se possível, deve-se alterar as definições manualmente.

Como encriptar as comunicações com o Facebook Messenger: Abre o *chat*, seleciona o nome da pessoa e clica em "Conversa secreta". Agora a troca de mensagens com esta pessoa é encriptada de ponta a ponta. Ninguém, além de ti e do teu parceiro de conversa, conseguirão ver as mensagens, nem mesmo o Facebook.



Dica
É possível reconhecer uma conversa encriptada pelo facto da interface do utilizador ser **cinzenta-preta**. Verás também um pequeno cadeado preto na imagem de perfil do teu parceiro de conversa.

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

4.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_04_01

Situação: O que deve ser tido em consideração quando se usam *apps* em *smartphones*, para nos protegermos e à nossa privacidade?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Ler a política de privacidade e os termos e condições de cada aplicação de forma crítica antes de a instalar.
- Se possível, não concordar com quaisquer *updates* de aplicações.
- Não utilizar fotos de perfil do próprio, dado que não é seguro. É melhor utilizar fotografias que encontradas algures na Internet, tiradas por outras pessoas.
- Controlar os direitos de acesso das aplicações e ajustá-los adequadamente.
- Utilizar um endereço de correio eletrónico real para se registar (por exemplo, constituído pelo primeiro e último nome verdadeiro).
- Fornecer apenas a informação sobre o próprio que for absolutamente necessária.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_04_02

Situação: O que podes fazer relativamente às definições de privacidade de aplicações populares como o WhatsApp e o Facebook Messenger para assegurar a tua privacidade?
Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa.

- Ao utilizar, por exemplo, o WhatsApp, em “Definições” e “Privacidade” é possível impedir que outros utilizadores vejam quando estive *online* pela última vez.
- Posso desativar, por exemplo, o WhatsApp de aceder aos meus contactos em Definições e Privacidade.
- Ao utilizar o WhatsApp, posso também desativar a confirmação de leitura ou bloquear contactos indesejados, clicando em “Definições”, “Conta” e “Privacidade”.
- Também posso utilizar o Facebook Messenger para ter conversas encriptadas com os meus amigos: para o fazer, vou ao respetivo *chat*, seleciono o nome da pessoa e simplesmente inicio uma “conversa secreta”.
- Para comunicar com contactos que estão bloqueados no WhatsApp, basta selecionar o nome da pessoa e iniciar uma "conversa secreta".

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

Fontes

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

Para relembrar

Resumo

Para a maioria de nós, o seu ***smartphone*** é uma parte integral da vida quotidiana. Por conseguinte, não nos devemos esquecer de proteger devidamente a informação privada e os dados contidos no telemóvel. Por exemplo, em caso de perda ou roubo do *smartphone*, faz sentido **usar um PIN seguro** (e não uma combinação de números como 1234) e um **bloqueio de ecrã**. Também é aconselhado considerar a instalação de algum tipo de **aplicação antirroubo**.

Os provedores de mensagens instantâneas como o **WhatsApp** estão a tornar-se cada vez mais populares. Contudo, ao usar estas ou outras aplicações, é preciso ponderar sempre **quais os direitos de acesso que se concede à aplicação** e ceder o mínimo de acessos possível, apenas os necessários.
Já alguma vez te perguntaste porque é que o WhatsApp é gratuito? Ao utilizar aplicações gratuitas, deves estar sempre ciente de que, se não tiveres de pagar pelo produto, normalmente **tu ou os teus dados são o produto**. Adicionalmente, existe o perigo de haver ***malware* escondido** em aplicações, especialmente se estas *apps* forem distribuídas gratuitamente na Internet e por fornecedores de aplicações pouco conhecidos. Outro risco de segurança é o facto de alguns provedores de comunicações *online* não **encriptarem a comunicação** (por exemplo, o Facebook Messenger).

A aquisição do WhatsApp pelo Facebook fez com que muitos utilizadores se tornassem mais críticos sobre as políticas de privacidade destes serviços. Por conseguinte, as aplicações estão constantemente a ser otimizadas no que diz respeito às suas medidas de proteção de dados. Por este motivo, faz sentido, utilizar sempre a **versão mais recente do WhatsApp**, por exemplo. Além disso, antes de usar quaisquer *apps*, deve **ler a política de privacidade da aplicação** em causa, verificar os direitos de acesso da mesma e ajustá-los, se necessário. Pode também ajustar facilmente **as definições de privacidade das aplicações**, tais como a visibilidade da imagem do perfil no WhatsApp ou o bloqueio de contactos indesejados.

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

As respostas corretas estão assinaladas a negrito

Situação: Que medidas podem ser tomadas para proteger o *smartphone* de acessos não autorizados?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Usar um PIN que seja o mais fácil de memorizar possível.
- **Bloquear o *smartphone* com um PIN, garantindo que não é uma combinação de números como 1234 ou 1111.**
- **Configurar um bloqueio de ecrã.**
- Instalar uma aplicação paga para estabelecer um número de identificação pessoal (PIN).

Situação: Quando chegas a casa de uma tarde de compras na cidade, apercebes-te subitamente que perdeste o *smartphone*. Que medidas podem ser úteis numa situação destas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Usar o Android Device Manager ou o iCloud para localizar o *smartphone.***
- **Instalar algum tipo de aplicação anti-roubo para este tipo de situações. Isto permite localizar o telefone, bloqueá-lo ou apagar os dados armazenados no *smartphone*.**
- Bloquear o cartão SIM para localizar o telemóvel posteriormente.
- **Bloquear o cartão SIM para evitar que alguém incorra em custos elevados ao usar o telemóvel perdido.**

Situação: Quais das seguintes afirmações sobre mensagens instantâneas são verdadeiras?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Cada vez mais pessoas utilizam os serviços de mensagens instantâneas para trocar mensagens de texto, enquanto que a comunicação via SMS tem perdido popularidade.**
- **As mensagens instantâneas são comunicações baseadas na Internet.**
- **As mensagens instantâneas permitem não só a troca de mensagens de texto, mas também a troca de ficheiros, áudios ou videochamadas.**
- Se muitas pessoas utilizarem os mesmos serviços de mensagens instantâneas ao mesmo tempo, normalmente demora alguns minutos até que o destinatário receba as mensagens.
- **Os serviços mais populares de mensagens instantâneas são o Facebook Messenger, o WhatsApp ou o Windows life messenger.**
- Os serviços mais populares de mensagens instantâneas são o Youtube, Twitter, WhatsApp e Google.

Situação: Queres usar o WhatsApp para comunicar com os teus amigos. O que deves ter em mente quando instalas a aplicação?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Aplicações como o WhatsApp requerem normalmente o pagamento de uma taxa única de utilização com antecedência.
- Para usar o WhatsApp, é necessário descarregar a aplicação e fazer um registo com o nome verdadeiro.
- **O WhatsApp acede a todos os contactos armazenados no *smartphone*.**
- **Para utilizar determinados serviços do WhatsApp, pode ser necessário permitir que a aplicação aceda às imagens, câmara, microfone ou dados de localização do telemóvel.**

- O WhatsApp acede automaticamente a todos os contactos armazenados no *smartphone*, às fotografias e aos dados de localização. Se não tiver acesso a estes dados, a aplicação não funciona.

Situação: Quando é que faz sentido ajustar as autorizações das aplicações e como é que é possível fazê-lo?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Basicamente, é possível verificar nas "Definições" quais das aplicações instaladas têm direitos de acesso e, se necessário, reduzir os acessos ao mínimo necessário.**
- Para perceber quais os direitos de acesso que uma aplicação tem é necessário contactar a tua operadora.
- **Se queres usar o Google Maps, por exemplo, deves permitir que a aplicação aceda aos dados da localização durante o uso.**
- Também é boa ideia permitir que o WhatsApp aceda aos dados de localização, uma vez que isso permite uma mais rápida transferência de mensagens.
- Uma vez que a maioria das aplicações não acarreta custos, normalmente não é possível restringir os direitos de acesso de cada uma das aplicações.

Situação: Porque é que os utilizadores de *apps* estão cada vez mais preocupados com a privacidade dos seus dados?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha única: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Porque as aplicações são cada vez mais usadas por um número cada vez maior de pessoas.
- Porque as aplicações são primeiramente desenvolvidas por empresas sediadas em países que não se preocupam com a proteção de dados e, por conseguinte, não existem regras vinculativas de proteção de dados para o tratamento de dados dos utilizadores. Um bom exemplo disso é o Facebook ou o WhatsApp.
- Porque as aplicações estão a tornar-se cada vez mais caras.
- **Porque alguns casos de violações da proteção de dados se tornaram conhecidos nos últimos anos.**
- Porque é impossível aos utilizadores compreender que direitos de acesso concedem aos vários provedores de aplicações.
- Porque os utilizadores estão a armazenar cada vez mais fotografias e outros ficheiros nos seus *smartphones* e, portanto, as capacidades de armazenamento vão esgotar-se em breve.

Situação: Quais são os riscos de segurança e consequências indesejadas que podem advir de serviços de mensagens instantâneas e outras aplicações?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **As aplicações de mensagens instantâneas estão ligadas a riscos de *phishing* ou transmissão de *malware* através de hiperligações clicáveis ou ficheiros transferidos.**
- **O *malware* pode estar presente especialmente em aplicações gratuitas de provedores de aplicações menos conhecidos.**
- Os custos ocultos bastante altos são um problema maior do que o acesso secreto a dados pessoais.
- A comunicação não encriptada, como ocorre, por exemplo, no WhatsApp é um grande problema de segurança.
- Os dados pessoais podem ser extraviados durante uma comunicação encriptada.

Situação: O que deve ser tido em consideração quando se usam *apps* em *smartphones*, para nos protegermos e à nossa privacidade?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Ler a política de privacidade e os termos e condições de cada aplicação de forma crítica antes de a instalar.
- Se possível, não concordar com quaisquer *updates* de aplicações.
- Não utilizar fotos de perfil do próprio, dado que não é seguro. É melhor utilizar fotografias que encontradas algures na Internet, tiradas por outras pessoas.
- Controlar os direitos de acesso das aplicações e ajustá-los adequadamente.
- Utilizar um endereço de correio eletrónico real para se registar (por exemplo, constituído pelo primeiro e último nome verdadeiro).
- Fornecer apenas a informação sobre o próprio que for absolutamente necessária.

Situação: O que podes fazer relativamente às definições de privacidade de aplicações populares como o WhatsApp e o Facebook Messenger para assegurar a tua privacidade?
Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa.

- Ao utilizar, por exemplo, o WhatsApp, em "Definições" e "Privacidade" é possível impedir que outros utilizadores vejam quando estive *online* pela última vez.
- Posso desativar, por exemplo, o WhatsApp de aceder aos meus contactos em Definições e Privacidade.
- Ao utilizar o WhatsApp, posso também desativar a confirmação de leitura ou bloquear contactos indesejados, clicando em "Definições", "Conta" e "Privacidade".
- Também posso utilizar o Facebook Messenger para ter conversas encriptadas com os meus amigos: para o fazer, vou ao respetivo *chat*, seleciono o nome da pessoa e simplesmente inicio uma "conversa secreta".
- Para comunicar com contactos que estão bloqueados no WhatsApp, basta selecionar o nome da pessoa e iniciar uma "conversa secreta".