ENJOY SAFER TECHNOLOGY™

GUIA DE

Segurança em redes sociais

Introdução

As redes sociais são parte dos hábitos diários de muitas pessoas. Tanto adultos como crianças, qualquer internauta usa ao menos uma rede social e a grande maioria deles participa ativamente em mais de uma. Estas plataformas são serviços de internet que permitem que os usuários gerem um perfil público no qual podem plasmar dados pessoais e informações de diferente cunho. O impacto que geraram é tal que para muitas pessoas, as redes sociais são os principais motivos para conectar-se na internet.

No entanto, a partir de seu uso constante, os usuários são expostos a um conjunto de ameaças tecnológicas que podem atentar contra suas informações, privacidade, dinheiro ou até mesmo sua própria integridade.

Frente a crescente tendência dos ataques tecnológicos que usa redes sociais como meio para seu desenvolvimento ou propagação, torna-se vital estar protegido e contar com um ambiente seguro no momento de usá-las.

Quais são os principais vetores de ataque aos que estão expostos os usuários destas redes? De que maneira os níveis de segurança podem melhorar? Quais são os novos problemas referentes à privacidade ao carregar excessivamente conteúdos distintos?
Este guia responderá a essas perguntas e mostrará as melhores práticas para alcançar uma maior proteção ao usar as redes sociais mais populares.

Índice

O alcance das redes sociais atualmente

O alcance das redes sociais atualmente

A seleção de redes sociais nas quais se baseia este guia se deve ao seu nível de penetração em diferentes países da América Latina e da quantidade de usuários que as usa.

+ 1650 MILHÕES DE USUÁRIOS

Sem dúvida é a maior rede social do mundo..

+ 310 MILHÕES DE USUÁRIOS

Este aplicativo inicialmente pensado para dispositivos móveis consolidou-se como o **rei do microbloging**.

+ 1000 MILHÕES DE USUÁRIOS

Principal plataforma utilizada para compartilhar vídeos.

+ 400 MILHÕES DE USUÁRIOS

Manipula imagens em um formato característico e vídeos de curta duração entre os usuários de sua própria rede.

+ 150 MILHÕES DE USUÁRIOS

Híbrido entre uma rede social e um aplicativo de mensagens; sua fama se dá pela nova forma de compartilhar imagens que se "autodestroem" depois de certo tempo

+450 MILHÕES DE USUÁRIOS

Baseada em contatos profissionais conhecidos, os usuários trocam diferentes tipos de informações que vão desde pesquisas de trabalho, até opiniões e artigos entre diferentes grupos temáticos.

Principais vetores de ataque

Principais vetores de ataque

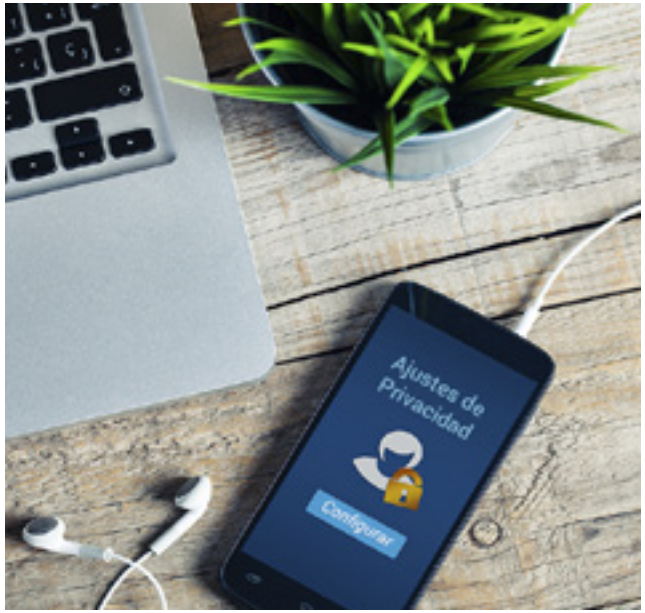
A Engenharia Social, definida como a arte de dissuadir as pessas,é um dos grandes pilares usados pelos ciberdelinquentes para executar diferentes tipos de ataques. Em muitos casos, a informação extraida nas redes junto a uma **má configuração de privacidade** pode ser a fórmula perfeita para gerar um chamariz atraente para a maioria parte das vítimas. Com relação aos incidentes, a diversidade de ataques pode ser categorizada principalmente em seis grandes grupos dependendo de sua natureza.

Infecções com malware

São arquivos com fins prejudiciais que, ao infectar um computador, realizam diversas ações, como o roubo ou sequestro de informações, o controle do sistema, a captura de senhas ou sessões ativas e até deteriorar o rendimento do dispositivo infectado. Worms, trojans e ransomware são as variantes mais conhecidas neste campo.

Particularmente no Facebook, houve várias campanhas de propagação de malware nas quais as técnicas de Engenharia Social foram o padrão comum. **Remtasu**,por exemplo, encontrava-se camuflado em ferramentas falsas para tomar o controle de contas alheias no Facebook. A campanha de Kilim, por sua vez, utilizava o serviço de mensagens enviando como chamariz um **falso vídeo** no qual finalizava instalando um complemento no navegador que comprometia a privacidade dos usuários. Além disso, a armadilha antiga ligada a **quem visita seu perfil** e inclusive algumas campanhas maliciosas que se relacionavam com serviços de mensagens, como o **WhatsApp**, também conseguiram se propagar por esta rede social.

A alta eficácia de propagação deste tipo de ameaças, origina-se em que uma vez que a conta da rede social é infectada, os códigos maliciosos a aproveitam para continuar dispersando-se entre os contatos da vítima..



Fraudes digitais

Igualmente a determinados códigos maliciosos, as fraudes digitais também se propagam nas redes sociais. Particularmente através do Facebook foram vistos casos de golpes vinculados a serviços de SMS Premium..

Por outro lado, os incidentes de **phishing** segum sendo uma das principais preocupações. Através de um e-mail falso, os ciberdelinquentes se fazem passar por uma entidade conhecida e convidam o receptor para acessar a um lik. Quando para a vítima parece estar no site real, no entanto, o domínio

que está visitando não pertenece à entidade conhecida e sua única função será capturar seu nome de usuário e senha. Dessa maneira, os ciberdelinquentes tem êxito com credenciais de acesso de muitas contas de redes sociais e, inclusive, entidades financeiras.

Como reconhecer um e-mail de phishing, um link falso ou um site falso?

Normalmente, estes e-mails chegam com um cabeçalho de usuário genérico, por exemplo, o clássico "Caro usuário"; outra característica muito comum é que ao posicionar o cursor sobre o link, aparecerá um novo endereço que é diferente do link que é exibido na tela Por último, deve-se verificar que a URL comece com o protocolo HTTPS, já que oferecerá mais segurança ao criptografar a comunicação com o site.

Roubo de informações

No uso diário das redes sociais, os usuários compartilham diversos dados de cunho pessoal que podem ser úteis para os atacantes. O roubo de informações nas redes sociais está relacionado diretamente com o roubo de identidade, um dos delitos informáticos que mais cresceu nos últimos anos.

Os dois vetores de ataque mais importantes para o roubo de informações são:

Engenharia Social

Aqui se busca o contato direto com a vítima, extraindo informações através do vínculo, da "amizade" ou qualquer comunicação que a rede social permita.

Informações públicas

Uma má configuração das redes sociais pode permitir que informações de cunho pessoal fiquem acessíveis além do que o usuário desejaria ou que lhe seria conveniente. Os cibercriminosos buscam este tipo de descuidos para ter êxito com tais informações.

Grooming

Consiste em ações deliberadamente empreendidas por um adulto com o objetivo de fazer amizade com um menor de idade e abusar sexualmente dele. As redes sociais são um espaço onde este tipo de riscos são muito presentes, já que os groomers podem se aproveitar do anonimato para fazer se passar por crianças e, assim, chegar até suas vítimas.

Ainda que seja certo que os pequenos aprendam com maior velocidade e estejam atualizados com os novos aplicativos e tecnologias, eles não percebem com a mesma naturalidade a maldade ou segundas intenções que um adulto desconhecido possa ter, que, em muitos casos, esconde sua identidade.

+ VER O GUIA DE PROTEÇÃO INFANTIL

Ainda que os pequenos aprendam com maior velocidade e estejam atualizados com os novos aplicativos e tecnologias, eles não percebem com a mesma naturalidade a maldade ou segundas intenções que um adulto desconhecido possa ter, que, em muitos casos, esconde sua identidade.

Cyberbulling

Implica na utilização de meios de comunicação digitais como as redes sociais, websites, fóruns, etc., com o fim de assediar e perseguir de forma premeditada a uma pessoa ou grupo. O cyberbullying se expande viralmente pela web e pode ser difícil de parar; por esta razão ele é invasivo e prejudicial.

As formas mais comuns são a difusão de falsos rumores, vídeos ou fotos humilhantes e a criação de perfis ou sites para agredir à vítima. Também pode ocorrer que o agressor se faça passar por outra pessoa para dizer coisas desagradáveis ou ameace a vítima com publicações de suas informações pessoais.

Sexting

Consiste no envio de conteúdos do tipo sexual, principalmente fotografias e/ou vídeos para outras pessoas por meios digitais.

Uma das redes sociais mais afetadas com este problema é o Snapchat, a qual permite o envio deste tipo de conteúdo com a ilusão de que estas informações se apagarão em poucos segundos. Porém, se este conteúdo cair nas mãos erradas, irá viralizar extremamente rápido, ou seja, irá se difundir massivamente sem nenhum tipo de controle nas redes causando um grande impacto social nos atores envolvidos..

As formas mais comuns são a difusão de falsos rumores, vídeos ou fotos humilhantes e a criação de perfis ou sites para agredir à vítima. Também pode ocorrer que o agressor se faça passar por outra pessoa para dizer coisas desagradáveis ou ameace a vítima com publicações de suas informações pessoais.

+ VER VÍDEO DE CYBERBULLYING

Práticas para alcançar um nível maior de segurança

Práticas para alcançar um nível maior de segurança

Frente a esse cenário de ameaças, o uso das redes sociais pode parecer perigoso. No entanto, se alguns conselhos e boas práticas forem seguidos, será possível utilizá-las e contar com níveis de proteção adequados para um uso correto e seguro dessas plataformas.

Como principais medidas se destacam: utilizar soluções de segurança, configurar corretamente os usuários nas redes sociais, utilizar quando for possível um segundo fator de autenticação e o protocolo HTTPS para navegação.

No entanto, a constante educação e o uso cuidadoso no momento da navegação sempre permitirão minimizar os riscos de forma importante.

Soluções de segurança

Sendo os códigos maliciosos a ameaça massiva mais importante, a utilização de um software antivírus com capacidades proativas de detecção e com uma base de assinaturas atualizadas é um componente fundamental para prevenir o malware que se propaga por redes sociais.

As ferramentas antispam e de firewall também permitem otimizar a segurança do sistema frente a esses riscos. Também é fundamental não usar um usuário com permissões de administrador no momento de navegar por essas redes, e que cada pessoa que use o equipamento tenha seus próprios perfis. Esta é uma forma de minimizar o impacto caso ocorra um incidente.

Finalmente, para monitorar e supervisionar o uso por parte dos menores de idade, existem ferramentas de controle parental que permitem bloquear sites indesejados, além de restringir certas faixas de horário (como quando a criança está na escola, por exemplo) ou, de plano, a quantidade de tempo que a criança usa as redes sociais..

Senhas

As senhas são a chave de sua identidade digital, por isso é extremamente importante que você as proteja. Você pode usar as recomendações que servem para proteger suas contas de redes sociais:

- Não use sua senha de redes sociais em outros sites de internet e nunca compartilhe-as..
- Evite incluir seu nome ou palavras comuns. A senha deve ser difícil de adivinhar.
- Evite usar computadores públicos para entrar em redes sociais. Lembre-se de encerrar a sessão, principalmente ao utilizar um computador compartilhado com outras pessoas.
- Pense duas vezes antes de clicar ou baixar qualquer conteúdo, lembre-se que pode ser algum sinal de Engenharia Social..

Configurações

Por padrão, nem sempre as configurações nas redes sociais são as melhores para sua segurança. Portanto, é recomendável dedicar um tempo razoável no momento de se cadastrar, além de revisar quais são as possíveis fugas de informação frente a uma má configuração do sistema em relação à **privacidade**.

Se possível, para uma maior segurança na sua conta, é recomendável configurar um segundo fator de autenticação; se você não está familiarizado com essa metodologia, consulte o **guia de dupla autentificação**.

A seguir, serão detalhadas as principais recomendações nas principais redes sociais utilizadas..

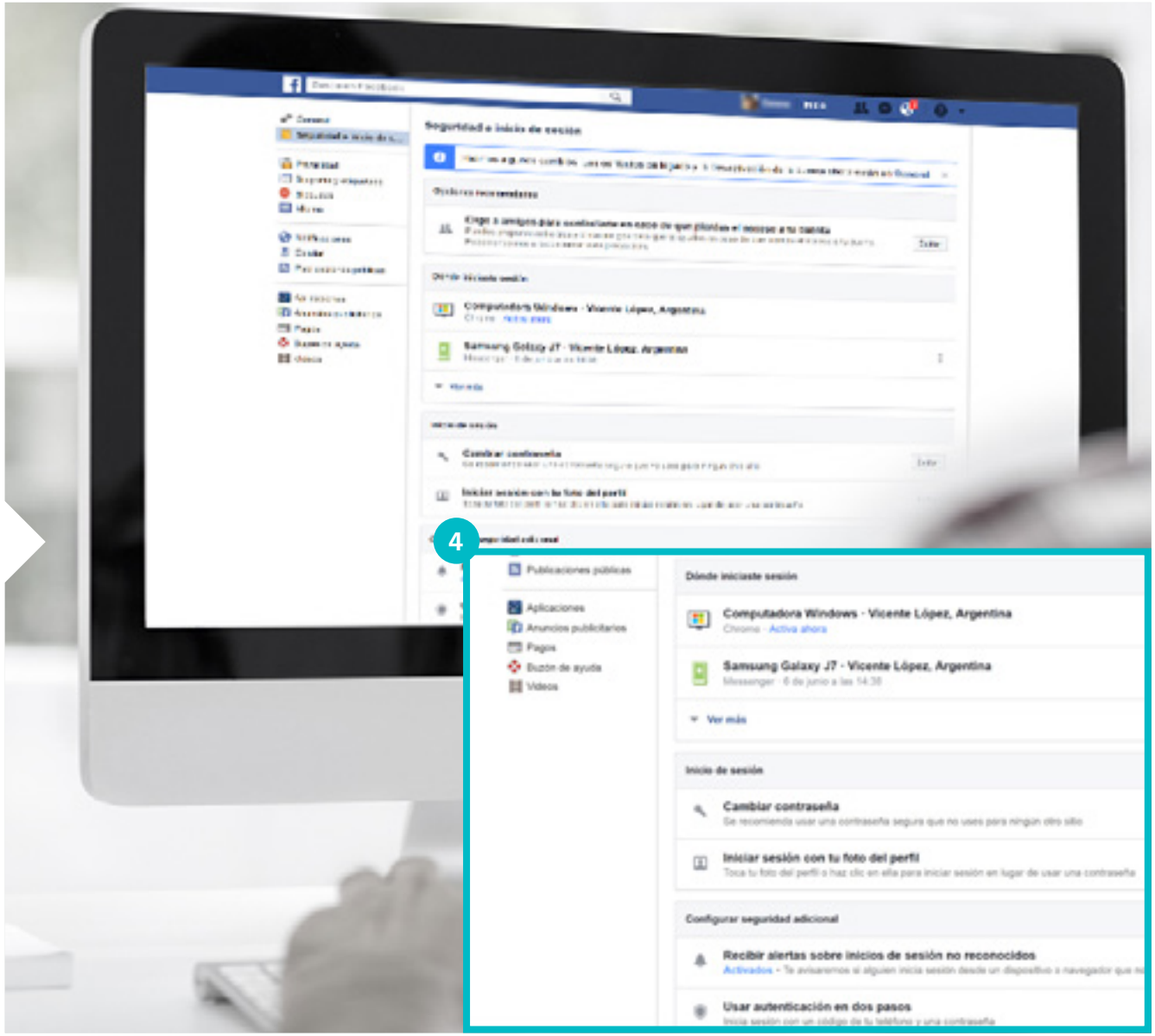
Facebook

Para analisar o estado da configuração nesta rede social, simplesmente dê três cliques, começando pela seta superior direita **(ref. 1)**, para então entrar em configurações **(ref. 2)** e, por último, em segurança e privacidade **(ref. 3)**, como você pode visualizar nas imagens.

Uma vez dentro de Segurança, poderão ser configurados valores que terão um impacto maior ou menor na segurança da conta; é recomendável que você se familiarize com isso..

É importante ativar as opções de alertas e aprovações de início de sessão. Se você tiver algum tipo de dúvida a respeito de outra pessoa estar entrando em seu perfil, você pode revisar as opções de "navegadores de confiança" **(ref. 4)** "onde você se conectou".

Por outro lado, controlar a privacidade terá maior relevância para elevar o grau de proteção do seu perfil.

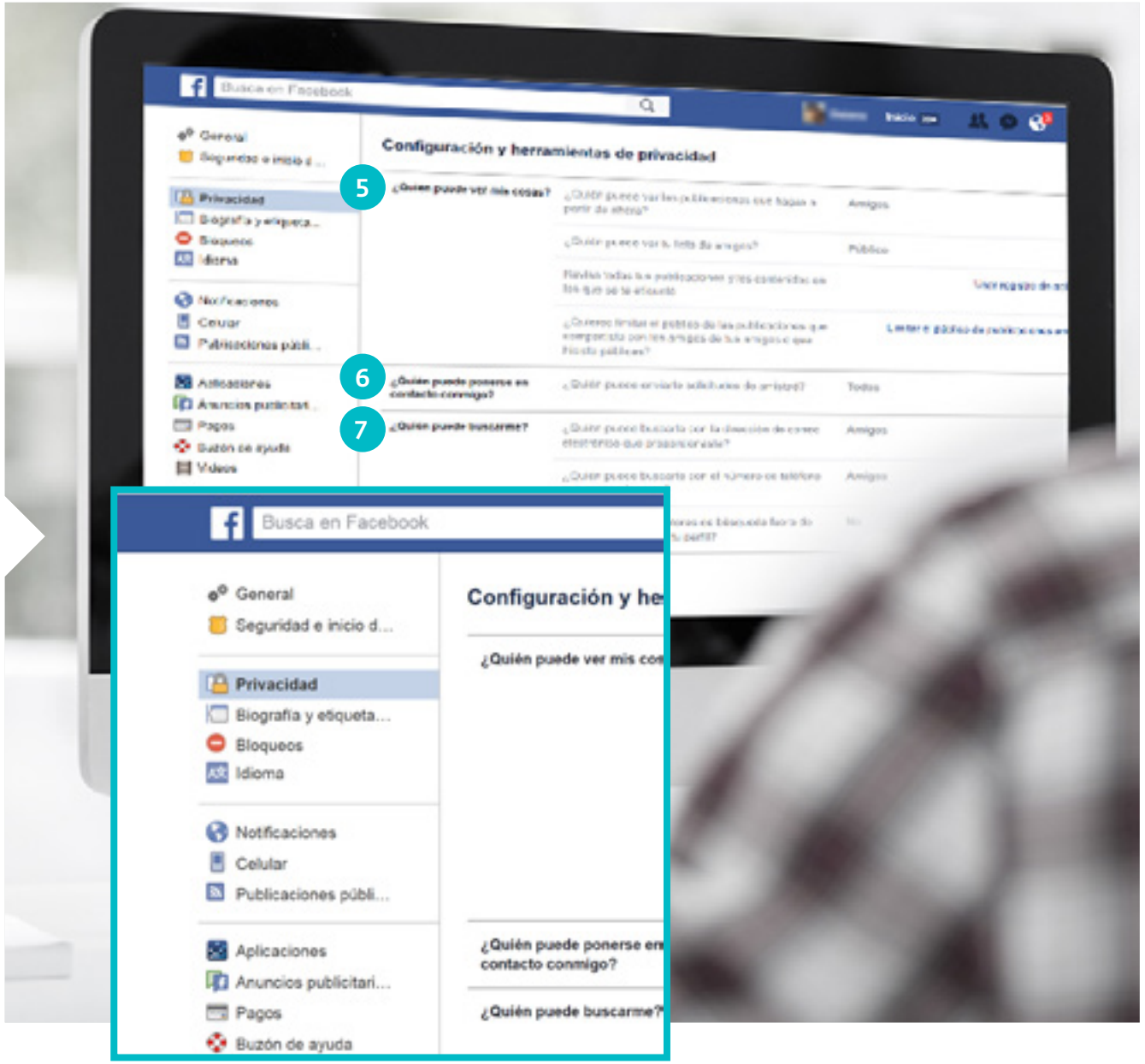


Estas são algumas opções com as quais você irá conseguir limitar a massificação das suas informações. Como você pode ver na imagem, o Facebook baseia sua privacidade principalmente em três pilares: quem pode ver suas publicações **(ref. 5)**,quem pode entrar em contato **(ref. 6)** e quem pode procurar você **(ref. 7)**.

Em relação a quem pode ver suas publicações, recomenda-se a opção "Somente eu", já que assim que revisar uma publicação, você poderá trocar o estado para "amigos". Dessa maneira, você protegerá sua privacidade no caso de publicar algo erroneamente.

Em relação a quem pode pesquisar você, aconselha-se evitar que os motores de busca encontrem seu perfil; dessa maneira, suas fotos publicadas não serão vistas nem encontradas simplesmente com uma pesquisa no Google.

Certamente, você não tem que adicionar gente que não conheça e, claro, se for menor de 13 anos, você não deveria usar essa rede social.

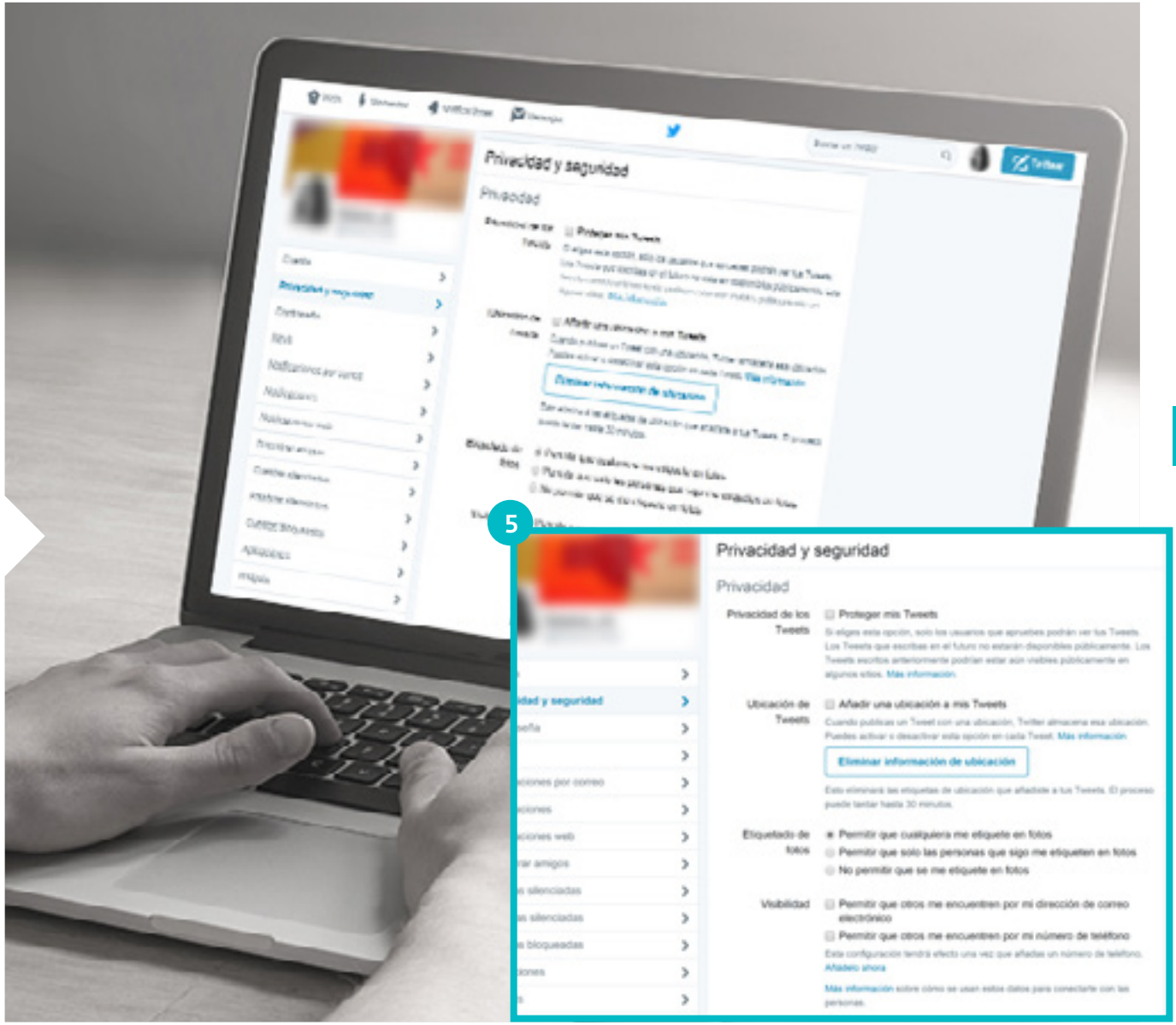


Twitter

Para revisar a configuração de segurança do seu perfil nessa rede social, você deverá clicar na sua imagem na margem superior direita **(ref. 1)**, depois em "configurações e privacidade" **(ref. 2)** e a seguir em "Celular" **(ref. 3)**.

Para reforçar a segurança, você poderá ativar a opção de verificação de sessão **(ref. 4)**, a qual enviará um SMS com um código para o telefone celular, o qual pedirá que você comece a usar o Twitter. Dessa maneira, caso sua senha seja roubada, não poderão entrar na sua conta.

Além disso, é muito importante que você cuide da sua privacidade **(ref. 5)**,portanto, você não deveria deixar que outras pessoas possam marcar você na sua foto. Por outro lado, se você escolher a opção "Proteger seus tweets", suas publicações serão vistas pelos perfis de pessoas que você autorizar. Por último, desativando a aba de adicionar localização, você estará preservando na maior parte sua superexposição nesta rede.



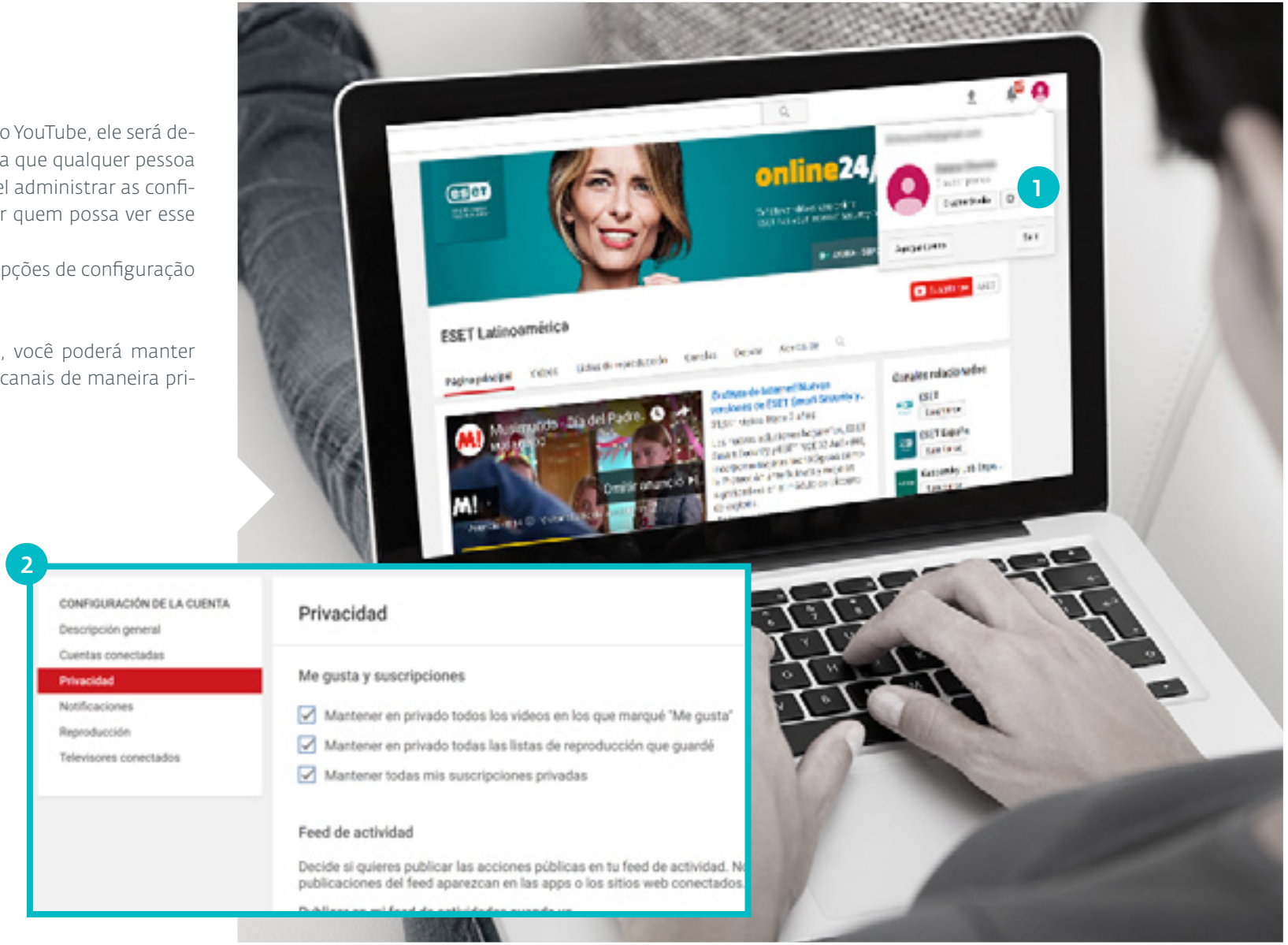
Instagram

Este aplicativo é usado para compartilhar imagens e vídeos de curta duração. Portanto, as medidas de segurança estão aplicadas a quem possa ver os conteúdos publicados. Na imagem seguinte, você poderá ver como configurar o perfil em modo "conta privada". Dessa maneira, quando alguém desconhecido quiser visualizar seu conteúdo deverá enviar uma solicitação para você.

Youtube

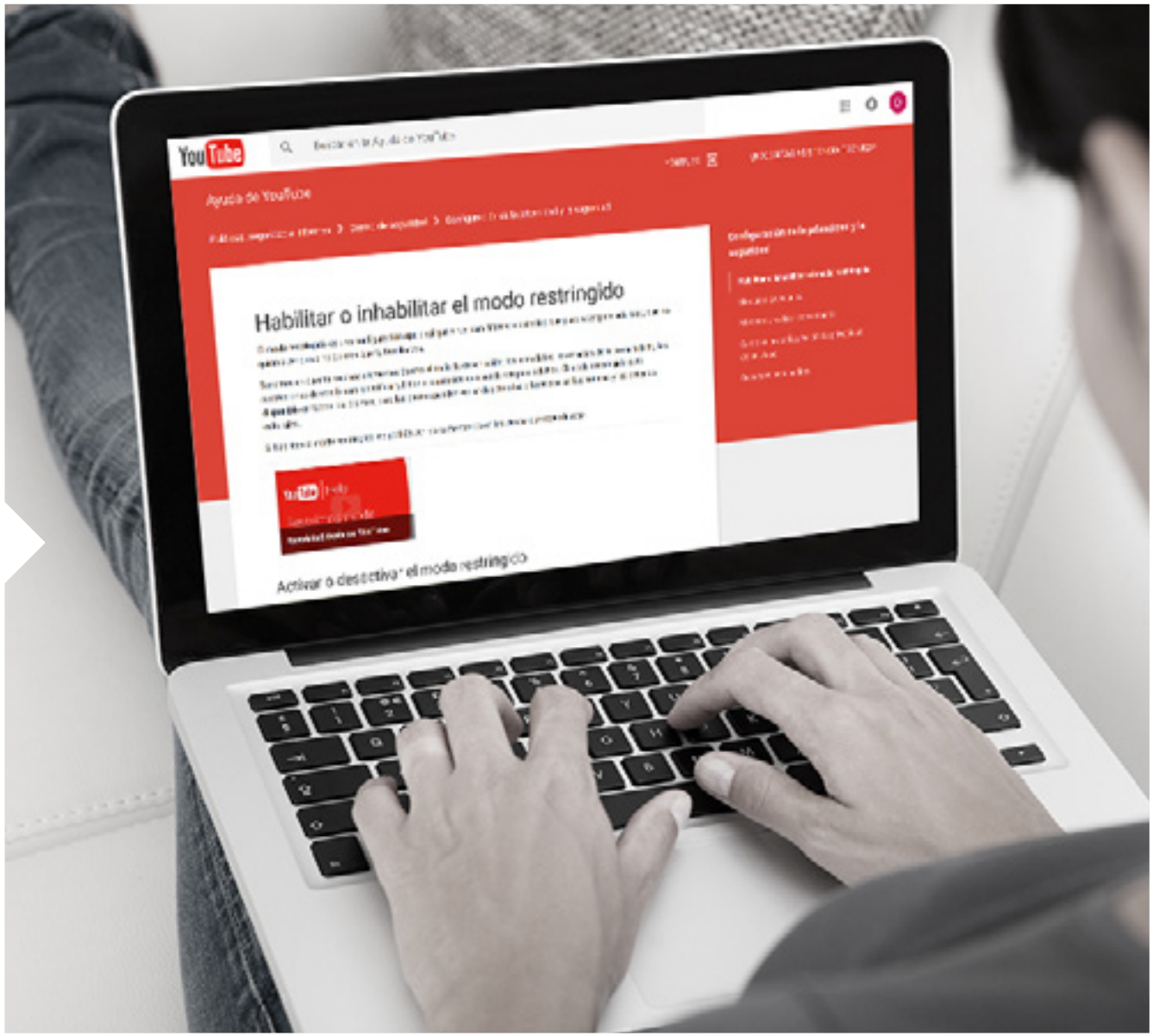
Por padrão, ao subir um vídeo para o YouTube, ele será definido como "público", o que significa que qualquer pessoa pode vê-lo. Neste sentido, é possível administrar as configurações de privacidade e controlar quem possa ver esse conteúdo.
Para fazê-lo, você deve entrar nas opções de configuração da sua conta**(ref. 1)**.

Entrando no menu de privacidade, você poderá manter seus vídeos e inscrições em outros canais de maneira privada **(ref. 2)**.



Além disso, você poderá habilitar o **modo restrito**, que é uma configuração que permite descartar conteúdo potencialmente indesejável que prefira não ver ou que você preferia que membros da sua família ou menores de idade encontrassem. Em outras palavras, é uma espécie de controle parental, especificamente para YouTube.

Tanto essa opção como outras interessantes que deveria observar, poderá encontrá-las no **Centro de segurança** da plataforma.

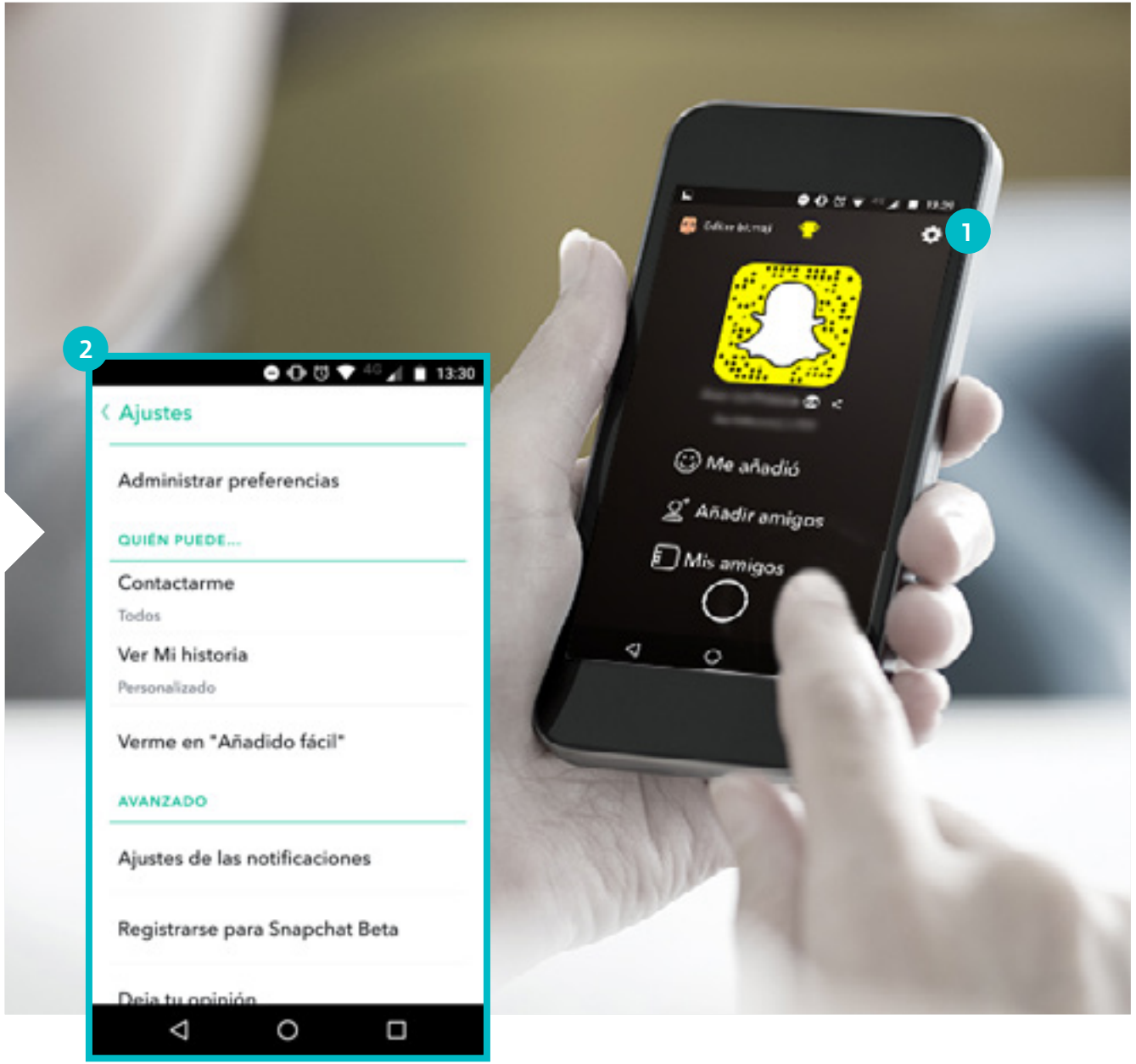


Snapchat

Um conselho importante relacionado ao uso deste aplicativo é que você não deve se esquecer que qualquer pessoa pode capturar uma tela de um snap ou simplesmente usar outra câmera para tirar uma foto. Por esse motivo, aconselha-se não enviar material que possa ser utilizado para perseguir a você ou outra pessoa.

Por outro lado, deslizando a tela até abaixo aparecerá uma nova interface de onde poderá configurar seus ajustes de segurança. Simplesmente clique no canto superior direito, como se vê na imagem **(ref. 1)**

Dentro do menu de ajustes, você poderá configurar opções de privacidade e relacionadas a quem pode entrar em contato e ver suas publicações **(ref. 2)**.



Conclusão

Sem dúvida, as redes sociais são um recurso valioso para os usuários. Desde contribuições na educação até as inter-relações de grupos mistos, fica claro que essas redes podem ser usadas com fins benefícos. Ainda que isso faça parte da interação social normal na atualidade, e necessário considerar que a internet e um mundo digital exposto, ou seja, que qualquer ação que se faça pode ter um impacto global e permanente.

Também pode ser perigoso publicar dados que possam identificar uma pessoa, como endereço, telefones, onde estuda ou trabalha, dias de férias, etc. Isso pode ser ainda mais complicado se voce possuir uma grande lista de amigos que não se conhecem pessoalmente.

Além disso, existe uma serie de ameaças que pode comprometer aos adultos e menores durante seu uso. Por esse motivo, recomenda-se nao subestimar o valor da privacidade e segurança nas redes, nem dos ciberdelinquentes. Dessa maneira, deve-se fazer um bom uso de ferramentas tecnológica, ter as configurações corretas , além de uma conduta adequada ao publicar conteúdos.

Dessa maneira, muito além do perfil do usuário e da natureza de seus conteudos compartilhados, sera possivel desfrutar das tecnologias e das redes sociais de forma segura.


ENJOY SAFER
TECHNOLOGY™