ENJOY SAFER TECHNOLOGY™

GUIA DE

Privacidade na Internet

Lucas Paus
Security Reasearcher

Introdução

Nos últimos anos fomos testemunhas da migração para a web 2.0 que, junto com o avanço vertiginoso da tecnologia, permitiu aos usuários subir e compartilhar todo tipo de conteúdo. Esta atividade ganhou cada vez mais popularidade, principalmente com a aparição das Redes Sociais que possibilitam subir informação para a internet, tais como localizações, fotos ou dados pessoais, a partir de um computador ou um dispositivo móvel. Da mesma maneira, é possível gerenciar contas bancárias e, incluso, realizar transações comerciais.

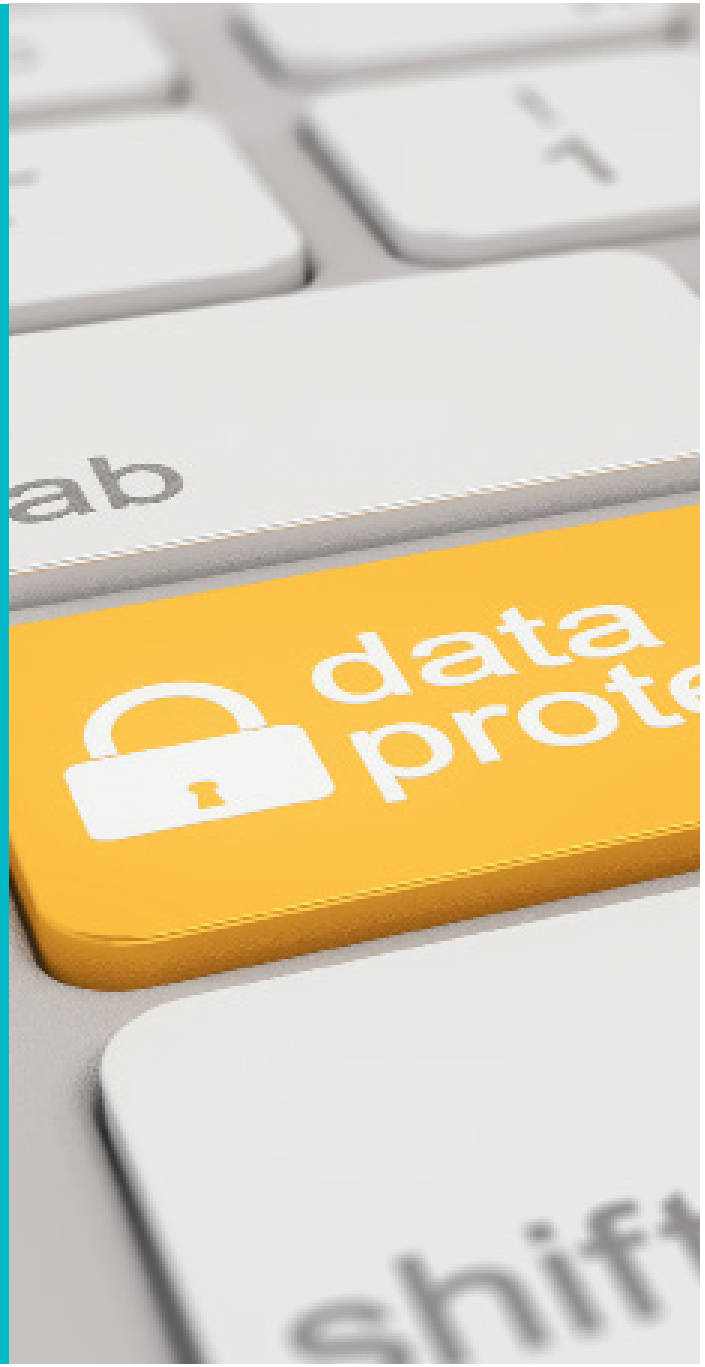
E Neste sentido, a grande concentração de informação sensível que se encontra disponível na internet pode tornar um usuário uma potencial vítima se não se tomam os cuidados necessários. Seguindo essa linha, realizamos este guia que ajudará a prevenir diferentes tipos de incidentes relacionados com a privacidade, a Engenharia Social e o roubo de informação.

Índice

O que é privacidade

“

A privacidade é aquilo que se leva a cabo em um âmbito reservado. Na internet poderia ser entendido como o controle que exercemos sobre nossa informação para limitar a quantidade de pessoas autorizadas a vê-la. Isso inclui dados pessoais, fotografias, documentos, etc”



Internet e a privacidade

A internet é uma ferramenta que permite, em conjunto com outras, a interação entre duas ou mais pessoas. Tal característica se vê refletida em Redes Sociais como Facebook e Twitter, onde as pessoas costumam compartilhar publicamente sentimentos, ideias, opiniões, noticias, fotografias, vídeos, etc. Sendo isso parte da interação social normal que se dá na atualidade, é necessário considerar que a internet é um espaço aberto ao mundo, portanto, qualquer ação que se faça pode ter um impacto global e permanente. Por exemplo, alguma publicação a qual uma pessoa possa se arrepender (como uma fotografia ou opinião) não somente poderá ser vista por milhões de usuários, como também será praticamente impossível apagá-la completamente da rede.

Também pode resultar perigoso publicar dados que possam identificar uma pessoa, como endereço, telefones, lugar de estudo ou trabalho, dias de férias, etc. Isto pode resultar mais complicado se se possui uma grande lista de amigos que não são conhecidos pessoalmente. Por tudo que foi mencionado, é de suma importância que antes de publicar algo, cada pessoa pense nas consequências que pode implicar a divulgação de informação sensível em sites públicos, os quais nem sempre se tem um controle direto.

Sendo a internet produto de grande alcance, massividade e outras características, é necessário compreender o que é a privacidade e como se pode aplicá-la corretamente nesse ambiente.

Ameaças

I - Oversharing

II - Protocolos inseguros

III - Códigos Maliciosos e Phishing

Ameaças que afetam a privacidade

Podemos reconhecer três tipos de situações que ameaçam ou põem em risco direto a privacidade da informação. A seguir, mencionamos cada uma e ao longo de todo o guia detalharemos com maior profundidade:

I

Oversharing: se dá ao compartilhar de maneira desmedida a informação. Se vê comumente em Redes Sociais e, com a ajuda dos smartphones, cada dia se faz mais notório. Na hora de planejar um ataque, um cibercriminoso pode nutrir-se de múltiplos dados, desde uma localização - como lugares onde você frequenta ou o escritório onde se trabalha - até detalhes dos contatos e amigos. Por esta razão, quanto mais se compartilha, mais exposto se estará.

II

Protocolos inseguros: se relaciona com a segurança na comunicação dos aplicativos. Em muitas ocasiões, utilizamos protocolos que realmente não põem foco em manter a segurança e privacidade dos usuários. Prevalecem outras questões como a funcionalidade e simplicidade no uso, deixando muitas vezes informações sensíveis expostas nas mãos de possíveis hackers.

III

Códigos maliciosos e phishing: há bastante tempo, os cibercriminosos geram códigos maliciosos com o fim de roubar informação financeira e credenciais de Redes Sociais para propagar campanhas maliciosas em nome das vítimas. Mesmo assim, espionam o comportamento de navegação das pessoas, de modo que possam gerar spam personalizado, tendo em conta os sites e ofertas que mais se visitam.

Por outro lado, se encontram os sites não autênticos, conhecidos como phishing, que roubam as credenciais de usuários distraídos que as colocam pensando estar em um site real. Entretanto, estes dados viajam até o hacker que ganha acesso às contas das vítimas, atentando contra sua privacidade e, muitas vezes, realizando atos fraudulentos.

Oversharing

I

Conceitos gerais em Redes Sociais

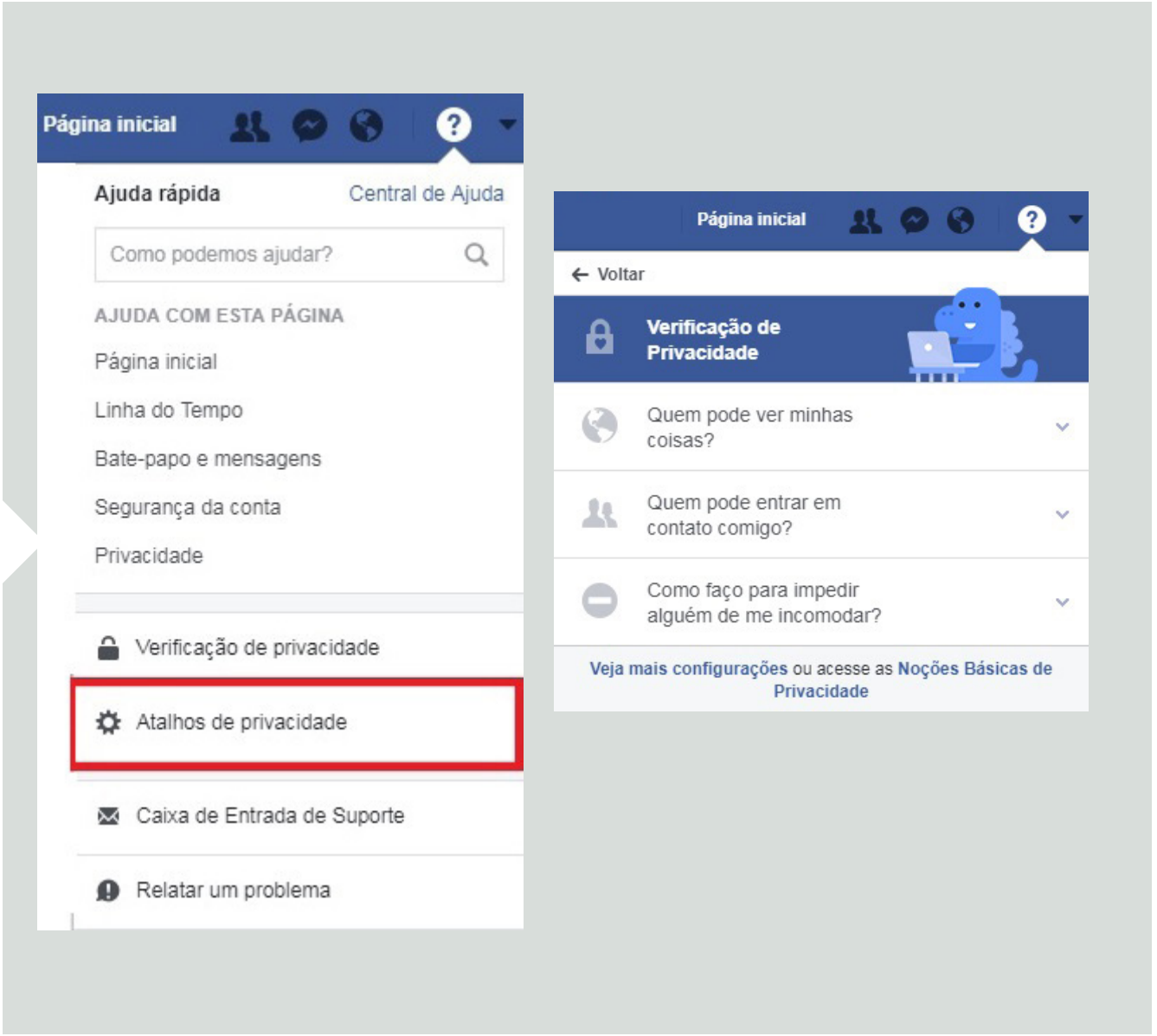
As configurações nas Redes Sociais não têm, por padrão, os níveis mais elevados quanto à proteção e segurança. Portanto, é recomendável dedicar um tempo prudente para mudá-las e, além disso, revisar de forma periódica quais são os possíveis vazamentos de informação ante uma má ou incorreta configuração de privacidade na plataforma.

Revisemos como fazê-lo nas principais redes:

Facebook

①

Na margem superior direita do aplicativo temos o ícone com ponto de interrogação, o qual nos servirá para revisar de forma sensata a privacidade do perfil, tal como se vê na seguinte imagem:

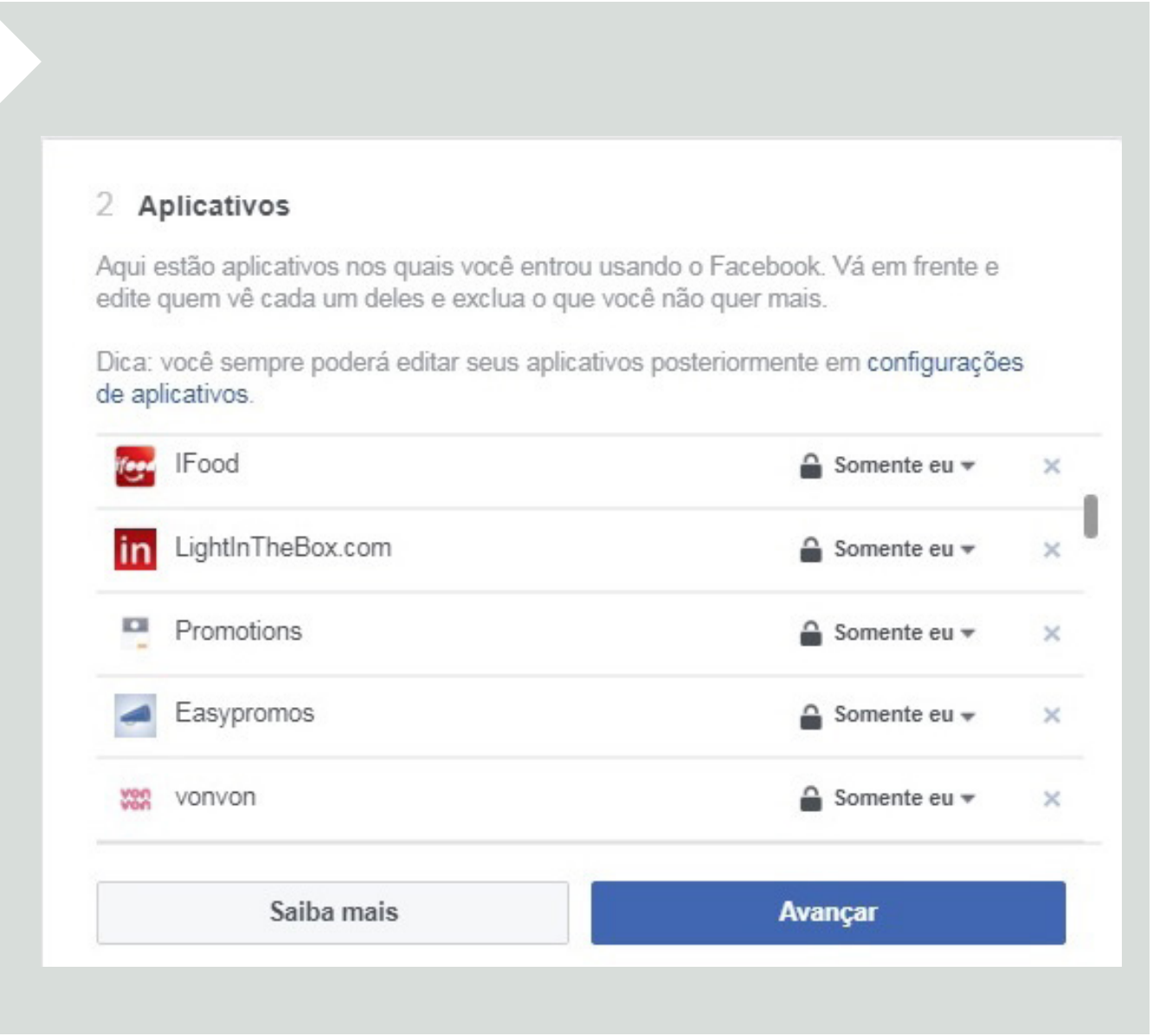


②

É importante revisar com quem se compartilha as publicações, quer dizer, que público terá acesso à informação. Isto é vital, pois recomendamos compartilhar a informação sempre com os amigos e, na medida do possível, tê-los classificados por grupos, como colégio ou clube. Na imagem seguinte, podemos identificar como mudar a configuração padrão e compartilhar conteúdos somente entre amigos.

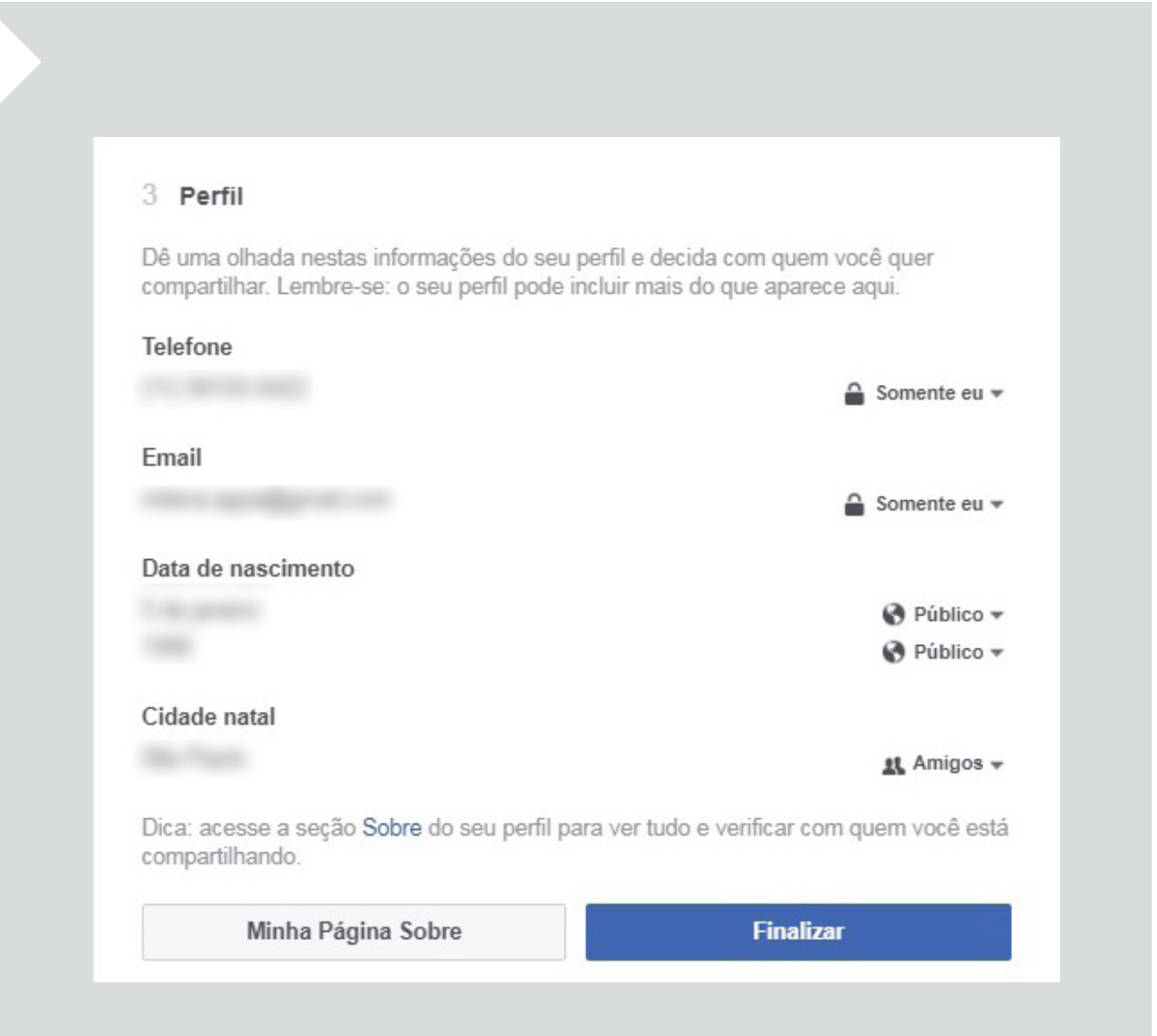
3

A seguinte operação é decidir quais aplicativos têm acesso ao perfil, já que muitos poderiam publicar informação em nome do usuário, por isso é vital que se leia e designe com atenção os controles de permissão. Na tela seguinte, observamos como podemos restringir os grupos de usuários que verão as mensagens dos aplicativos a partir do perfil:



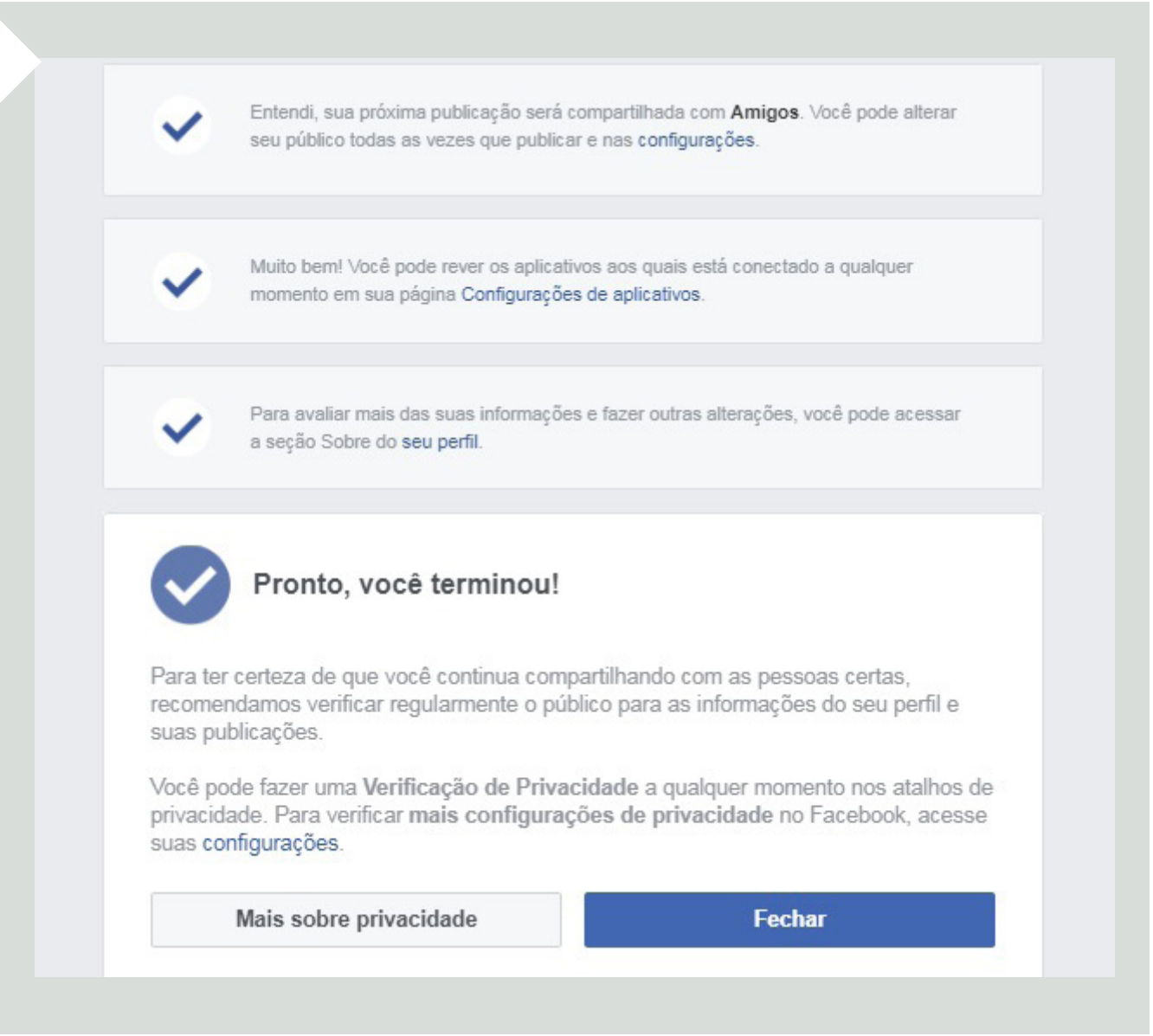
④

Este passo está relacionado com a informação pessoal que se compartilha diretamente no perfil. Neste ponto, é importante considerar o fim específico de compartilhar dados, como endereço, telefone ou e-mail. Como dissemos anteriormente, se deve ter em conta que quanto mais informação pessoal for compartilhada, maior será o risco de sofrer ataques, como por exemplo, de Engenharia Social.

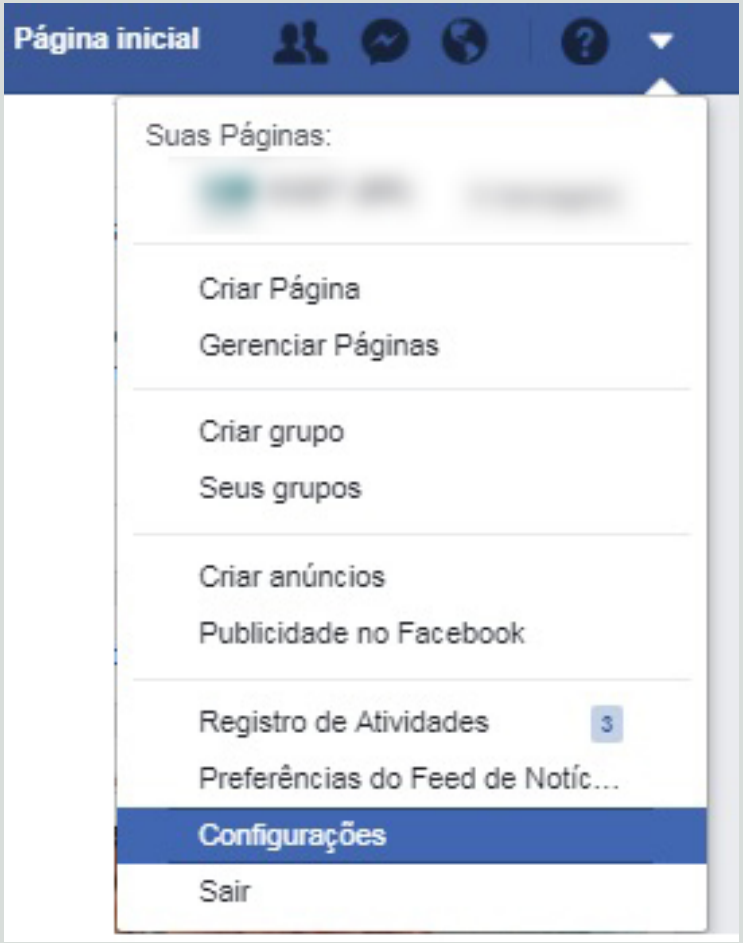


⑤

Deste modo, finalizamos o processo de comprovação rápida de privacidade em um perfil do Facebook.



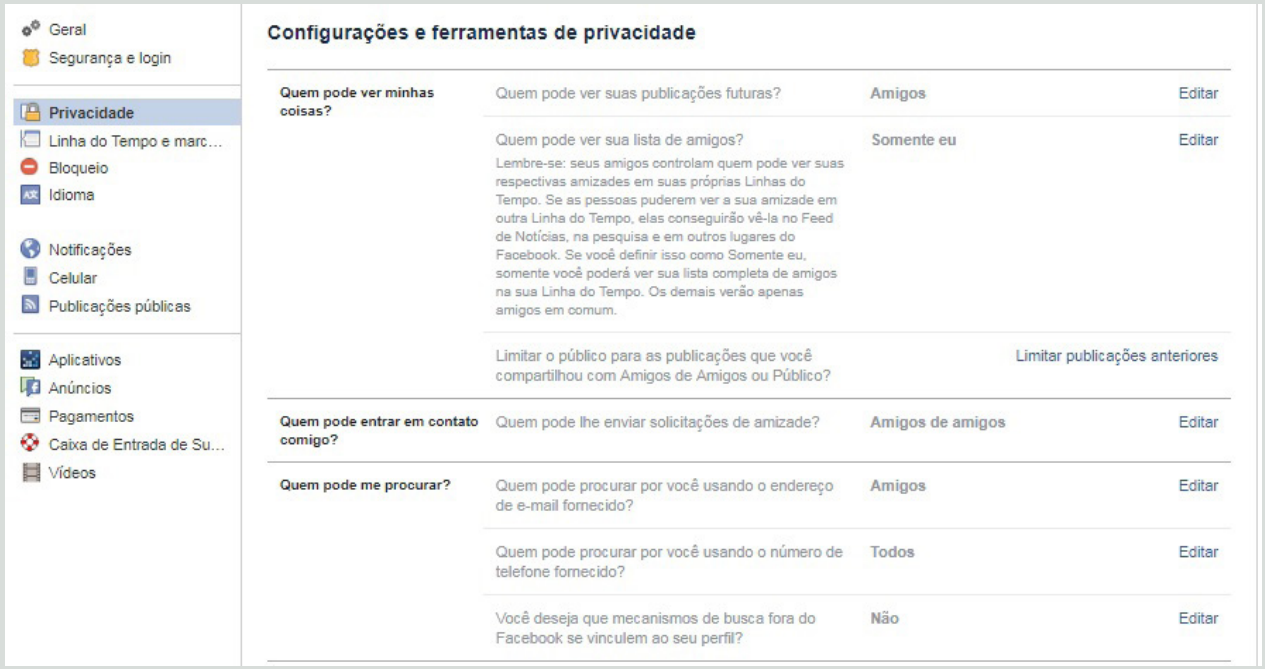
Já vimos como em 5 passos um usuário poderá revisar os parâmetros e níveis de privacidade. Entretanto, se quiser realizar uma análise mais profunda, deve-se ter em conta as seguintes opções a partir do menu de configuração:



A partir deste ponto, o Facebook permite escolher as seguintes opções, tal como se vê na imagem posterior:

- Quem pode ver aas publicações por padrão.
- Revisão das publicações que podem marcar um usuário.
- Quem pode entrar em contato com o usuário, especificamente sobre solicitações de amizade e mensagens privadas. .
- Quem pode procurar um usuário, precisamente configurando parâmetros como e-mails, números de telefone ou mecanismos de busca que possam relacionar-se com o perfil.

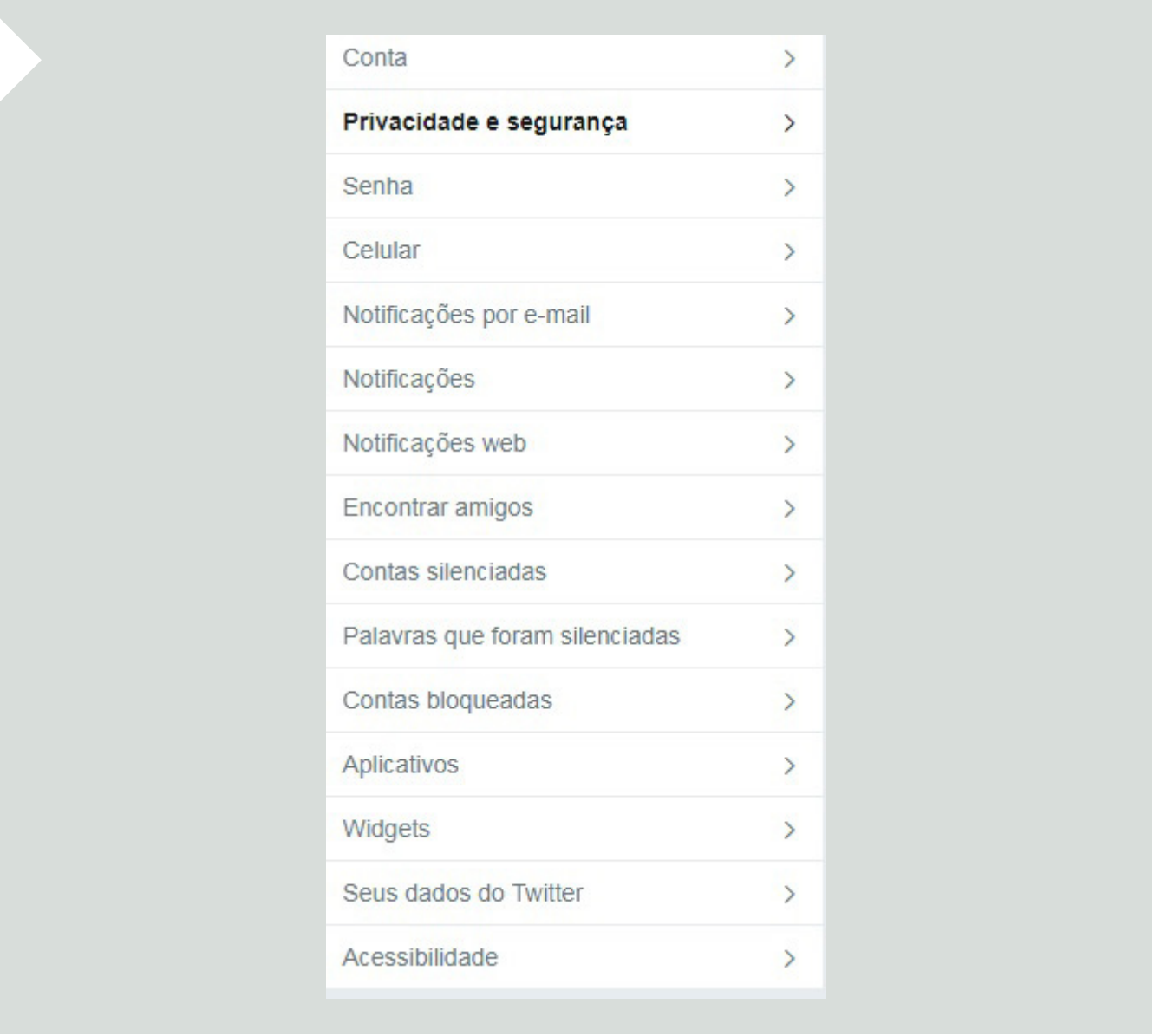
Recomendamos usar a opção "somente amigos"



Por outro lado, na aba „Biografia" e „Marcação" se poderão configurar questões que também estão vinculadas com a Privacidade. Algumas delas são: poder marcar um usuário, quem verá as marcações, a opção de que outros usuários possam escrever no mural e, inclusive, receber sugestões sobre marcação. Mesmo que cada configuração possa ser personalizada para cada perfil, recomendamos que se utilize a imagem seguinte como guia:

Twitter

Twitter é outra Rede Social muito utilizada, vinculada aos smartphones desde seu nascimento, que permite melhorar a privacidade dos usuários mediante algumas ações que veremos a seguir:



①

Dentro da aba „Privacidade" é possível selecionar a opção de não permitir que marquem alguém em sua conta, de deixar os tweets visíveis somente para pessoas que se encontrem na lista de contatos e, inclusive, não revelar a localização geográfica de onde se tweetou. A seguir, vemos os menus de cada opção:

2

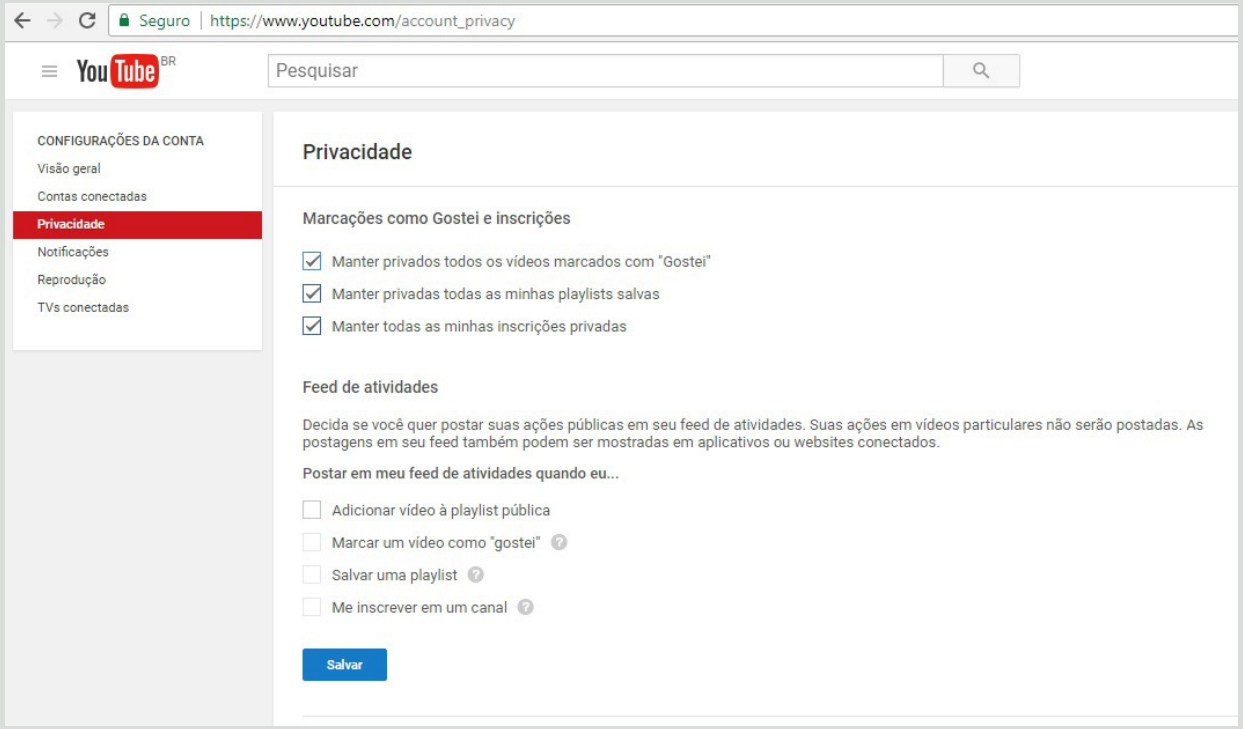
Além disso, podemos personalizar a opção de não permitir que o usuário seja encontrado por seu e-mail, tal como se vê a seguir:

Como no caso do Facebook, no Twitter também é recomendável verificar quais aplicativos têm acesso ao perfil de usuário. É aconselhável revogar ou desabilitar acesso aos aplicativos que sejam suspeitos ou sejam diretamente desconhecidos.

YouTube

Para finalizar, vejamos o último exemplo com o YouTube, uma Rede Social que nos permite subir vídeos e compartilhá-los.
Como se pode ver na imagem seguinte, o usuário tem a opção de manter os vídeos, as listas de reproduçãzo e, inclusive, as inscrições a outros canais como privados:

Além disso, se vídeos próprios são feitos, sempre é importante ter cuidado com a informação pessoal que se pode chegar a revelar neste conteúdo e se assegurar que eles não sejam uma porta aberta para ser contactado através de outra rede social com o objetivo de obter mais informação por parte de um hacker. Também se deve ser cuidadoso com os comentários incluídos nos vídeos, em que se convida para visitar sites de reputação duvidosa e que poderiam valer-se dos interesses do usuário que cria o video.



Metadatos

Comumente, se define metadados como um conjunto de dados sobre dados. Se o levamos à vida diária, um exemplo poderia ser o seguinte: se o dado em questão é um livro, a ficha que poderíamos ter sobre esse livro em uma biblioteca seriam os metadados, quer dizer, seu autor, data de publicação, editorial e demais especificações do livro (dados).

Para o caso de arquivos como fotos, música e documentos do Office, estes arquivos também trazem consigo metadados que, em muitas ocasiões, servirão para buscar um arquivo criado em uma data específica, de um autor determinado e, inclusive, saber em que qualidade se encontra um arquivo de áudio.

Entretanto, há momentos em que, através de imagens, se pode conhecer uma posição geográfica (mediante coordenadas GPS) no caso dos smartphones, ou subindo algum arquivo Office para a nuvem se pode ver o nome de usuário de um equipamento. É por isto que se deve ter um cuidado especial entendendo que a informação que subimos para a internet pode conter (ou fornecer) mais dados que meramente o que se vê em uma foto ou se mostra em um arquivo.

SSe na atualidade a maioria das Redes Sociais elimina os metadados, não se pode saber de forma segura se futuras redes também o farão, por isso nos parece importante ressaltar sua existência e os possíveis perigos que trazem emparelhados.

Protocolos inseguros

II

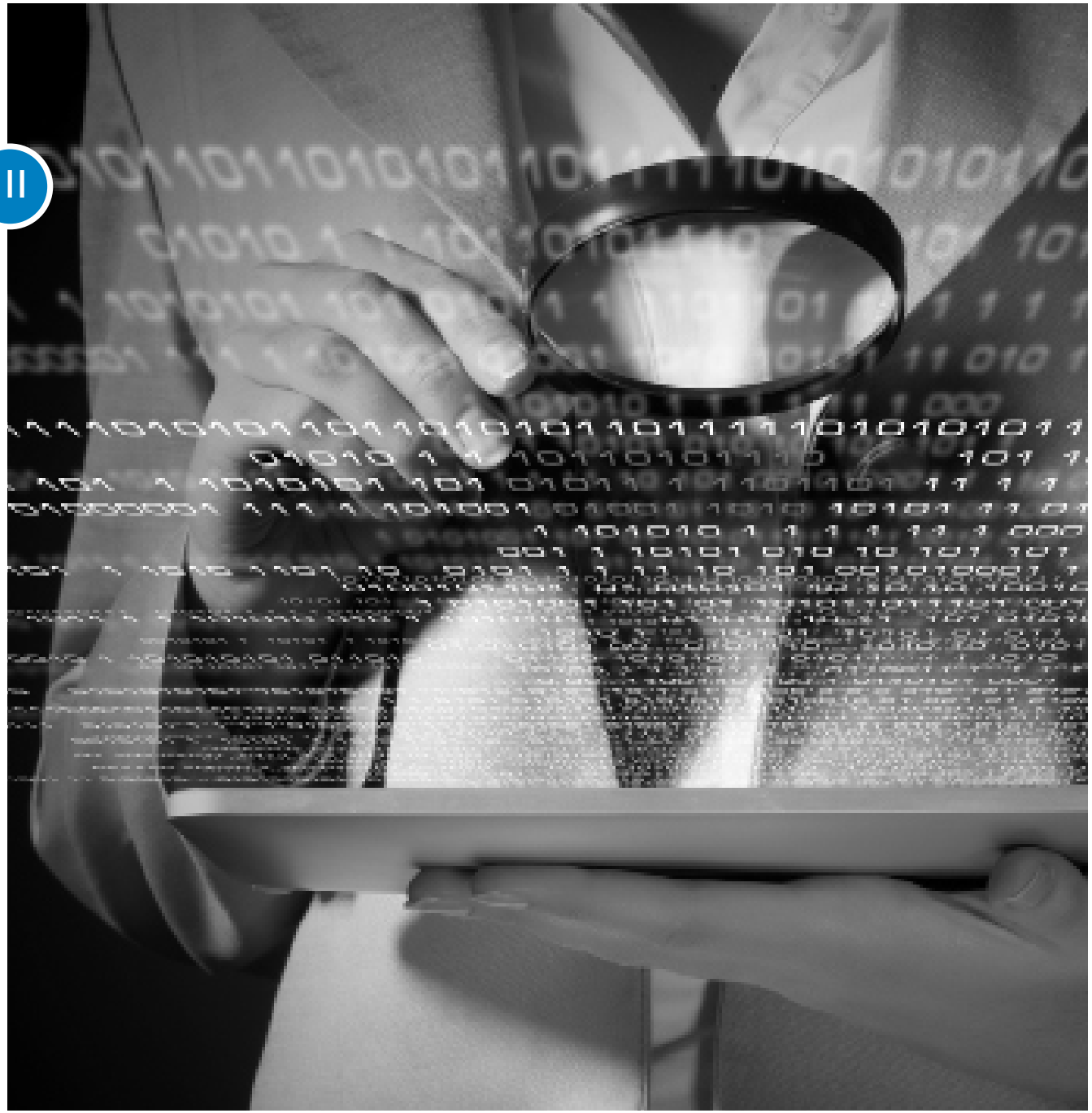
Precaução ao conectar-se em redes públicas

Cada vez que o usuário se conecta a uma rede Wi-Fi, o Windows ou alguns firewalls perguntam se se trata de uma rede doméstica, corporativa ou pública. É importante, como primeira medida, selecionar sempre "rede pública", para que se adotem configurações mais restritivas de segurança, especialmente no que diz respeito a arquivos compartilhados e acesso ao sistema. Se não se tem em conta os controles de segurança pertinentes, é recomendável evitar o uso de serviços que requeiram informação sensível em conexões Wi-Fi compartilhadas ou públicas.

Além disso, se deve levar em conta que ao conectar-se em redes de terceiros, não se sabe quais outras pessoas estão conectadas na mesma rede e nem suas intenções. Portanto, se deve tomar os mesmos cuidados que se tomaria em redes públicas.

Códigos maliciosos

III



Códigos Maliciosos

Durante estes últimos meses identificamos diversos ataques que utilizam as Redes Sociais como método de propagação. Entretanto, os métodos clássicos de infecção, como o envio de e-mails, todavia estão na ordem do dia e, em conjunto com técnicas de Engenharia Social, seguem enganando os usuários para conseguir infectá-los com malware.

A aparição de códigos maliciosos em Smartphones já não é uma novidade e daqui a pouco se tornarão en uma das plataformas com maior crescimento para o cibercrime. O Android encabeça o ranking de maiores ameaças encontradas vinculadas a códigos maliciosos. Contudo, todas as plataformas móveis estão em maior ou menor medida expostas ao malware que se propaga na internet e em repositórios de aplicativos não oficiais.

Além disso, a aparição de novos tipos de campanhas de propopagação de botnets, trojans ou keyloggers que podem ver-se ligados a noticias atuais ou personagens populares são utilizados como chamariz para atrair a atenção de suas vítimas.

Com estes tipos de infecção, os cibercriminosos adquirem acesso às chaves pessoais e informação sensível contida nos equipamentos. Neste sentido, utilizando uma solução completa de segurança, é possível prevenir proativamente as infecções contra diferentes tipos de malware e, deste modo, cuidar da privacidade dos dados. Para que esta barreira seja eficaz, é de vital importância manter atualizado o sistema operacional, os aplicativos que se utilizam e, claro, a solução de segurança.

Conselhos para cuidar da privacidade na Internet

Em segurança não existe uma só regra de ouro para proteger-se contra todos os possíveis incidentes que possam afetar a privacidade. Mas, pensando nos dez conselhos seguintes é possível minimizar em grande medida os riscos de ser vítima deste tipo de ataque:

- Evitar entrar em links suspeitos ou em sites de reputação duvidosa.
- Evitar utilizar sites que gerenciem informação sensível sem cadeado de segurança (HTTPS).
- Evitar realizar operações financeiras ou gerenciar as redes sociais a partir de redes Wi-Fi abertas.
- Evitar colocar informação pessoal em formulários de origem duvidosa.
- Utilizar e manter sempre atualizada a solução de segurança.
- Atualizar o sistema operacional e os aplicativos periodicamente.
- Tomar um tempo para configurar corretamente a privacidade das contas nas Redes Sociais.
- Aceitar somente contatos conhecidos e evitar o exceso de informação no perfil.
- Baixar aplicativos a partir de sites e repositórios oficiais.
- Evitar a execução de arquivos suspeitos provenientes de e-mails.

Conclusão

Ao longo deste guia, foi aprofundada a importância de contar com um gerenciamento ótimo da informação que se compartilha nas Redes Sociais. Sendo conscientes dos perigos de não gerenciar corretamente a privacidade e modificando os perfis por padrão, se contará com uma camada a mais de proteção nas plataformas, contribuindo assim para a proteção da informação.

Considerando que cada vez se gerencia mais informação sensível nas contas, resulta lógico que os cibercriminosos destinem maiores recursos à investigação e geração de códigos maliciosos para roubar as credenciais, conseguir acesso a informação do perfil e, finalmente, ter uma base mais robusta para seus ataques de Engenharia Social.

Do ponto de vista técnico, é possível reduzir este tipo de ataque, sempre e quando se conte com a participação e o compromisso dos usuários em todo o processo de proteção, sobretudo para evitar incidentes ligados a temas de privacidade. Para solucionar este inconveniente, é necessário que todos compreendam a importância do cuidado da privacidade como método de proteção. Aprendendo a configurar diferentes serviços e aplicativos disponíveis na internet de maneira correta, os dados não somente estarão mais seguros, como também se poderá aproveitar mais a tecnologia e tudo o que ela tem para oferecer.

www.eset.com.br

/EsetBrasil @ESET_Brasil /company/eset-brasil