Configurações de Segurança para Dispositivos Móveis
Google Android 6.0 (Marshmallow)
Apple iOS 10

Carlos Henrique G. de Araújo

13 de outubro de 2016

Sumário

Prefácio

Este pequeno livro detalha um conjunto de recomendações que visam tornar mais seguros os smartphones e tablets que executam o sistema operacional Android ou iOS. O objetivo dessas recomendações é tornar estes aparelhos mais seguros contra acesso indevido, vazamento de informações confidenciais, etc. A versão do sistema operacional Android que será tratada neste trabalho é a 6.0, também conhecida como Marshmallow. E a versão do sistema operacional iOS será a 10.0

Este trabalho foi originalmente concebido para ser lido pelo maior número de pessoas possível, desde como administradores de sistemas até usuários finais curiosos e entusiastas da área de segurança ou dos sistemas operacionais móveis.

Como este livro é organizado

O livro é composto por duas partes - Android e iOS - com quatro capítulos cada, que abrangem desde recomendações básicas até as mais específicas e avançadas. Segue logo abaixo uma descrição desta categorização.

As recomendações básicas são práticas e prudentes, fornecem um claro benefício em relação à segurança, e geram um impacto mínimo na usabilidade do dispositivo móvel, seja ele Android ou iOS.

Já as recomendações avançadas destinam-se a dispositivos nos quais a segurança é primordial, atuam em sua maioria como medidas de defesa em profundidade, e podem impactar significamente a usabilidade do dispositivo.

Em cada capítulo, as recomendações de segurança são apresentadas textualmente, e separadas em itens. Cada item é composto por:

- um título
- uma breve descrição, detalhando o item e seu propósito
- instruções detalhadas, explicando como realizar a configuração a fim de que o propósito do item seja alcançado

Por que LaTeX?

Caso o leitor tenha visualizado os arquivos utilizados para se criar este documento, terá percebido que eles não foram escritos em Word, LibreOffice, ou HTML. Eles foram escritos utilizando-se o LaTeX

Para quem não conhece, o LaTeX (Lamport TeX) é um processador de textos e uma linguagem de marcação de documentos criado por um cientista da computação americano chamado Leslie Lamport. Ele se baseou em um outro processador de textos, chamado TeX, este criado por um cientista da computação americano chamado Donald Knuth.

Inicialmente criado para a elaboração de textos acadêmicos da área de ciências exatas, hoje em dia o LaTeX é usado na área econômica e até política.

Decidiu-se escrever este trabalho em LaTeX devido a algumas vantagens que ele oferece, tais como:

- textos em LaTeX são escritos em texto plano, mas a ferramenta possui compiladores de conversão para diversos outros formatos: DVI, PDF, HTML, RTF, etc.
- ele possui suporte à modularização do texto, o que permite escrever capítulos e seções em arquivos fisicamente separados
- pode-se editar textos escritos em LaTeX em diversos softwares, desde o vim (Linux) até o TeXnicCenter (Windows)
- não importa qual a plataforma (Windows, Linux, Mac OS, etc.) utilizada, o texto resultante será sempre o mesmo

Existem, porém, algumas situações em que o usar o LaTeX pode se tornar desvantajoso. Para escrever documentos que necessitam de recursos visuais mais sofisticados, por exemplo, talvez o LaTeX não seja a melhor opção.

Parte I

Google Android 6.0 (Marshmallow)

Capítulo 1

Introdução

Este capítulo tem o objetivo de definir algumas premissas básicas, antes de se iniciar com as recomendações de segurança. A primeira delas é que o sistema operacional Android pode ser encontrado em uma gama diversa de aparelhos, como smartphones e tablets. Por isso, com o objetivo de simplificar a nomenclatura utilizada, tais equipamentos serão referenciados daqui por diante como dispositivos Android.

Todas as recomendações aqui descritas foram testadas em um smarphone Moto E, de segunda geração com 4G (LTE). As instruções das recomendações de segurança foram todas criadas com base na interface de usuário deste dispositivo. No caso dele, todas recomendações listadas sempre têm início pressionando o botão Aplicativos para em seguida, pressionar o botão Configurar. Segue abaixo a localização de cada um destes botões.

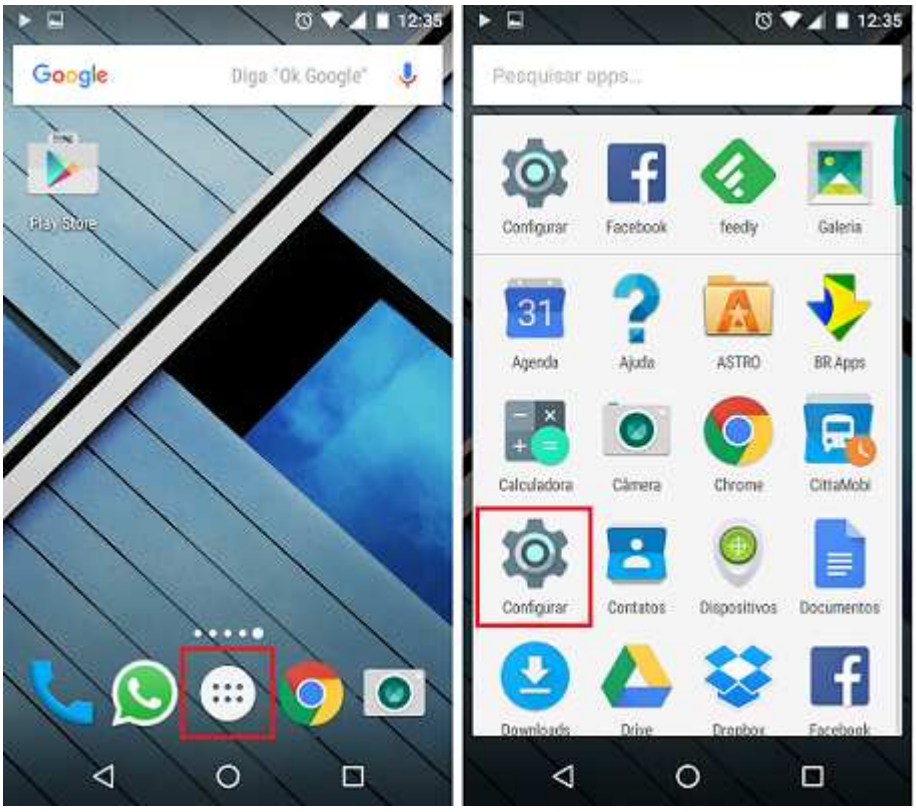

Figura 1.1: O botão Aplicativos e o botão Configurar, ambos destacados em vermelho

Como a interface varia conforme os dispositivos Android, devido à customização do sistema por parte de alguns fabricantes e operadoras de celulares, algumas instruções talvez não se apliquem diretamente ao dispositivo utilizado pelo leitor. Um exame mais detalhado nas configurações do dispositivo por parte do usuário, deve resolver este problema.

Também é necessário enfatizar que estas recomendações tratam da versão 6.0 do sistema Android (apelidada de Marshmallow). O leitor pode verificar se esta é a versão presente em seu dispositivo seguindo as instruções logo abaixo.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Sistema
4. Pressionar Sobre o telefone
5. Verificar se Versão do Android é 6.0 ou superior

Figura 1.2: A versão presente no dispositivo usado para testes, destacada em vermelho

Vale lembrar que o autor não se responsabiliza por eventuais danos causados em dispositivos Android decorrentes da aplicação das configurações recomendadas aqui. Por isso, é sugerido que, se possível, estas recomendações sejam aplicadas inicialmente em aparelhos de teste para, apenas depois, serem aplicadas em outros dispositivos.

Realizar backups das informações contidas no dispositivo também é uma prática recomendável para a recuperação de informações importantes, caso ocorram eventuais problemas. Seguem logo abaixo instruções para a realização de backups em dispositivos Android:

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Fazer backup e redefinir
5. Pressionar Backup dos dados
6. Ativar o backup dos dados
7. Voltar à tela anterior, e ativar a Restauração automática
8. Na mesma tela, Em Conta de backup, definir a conta em que o backup será realizado

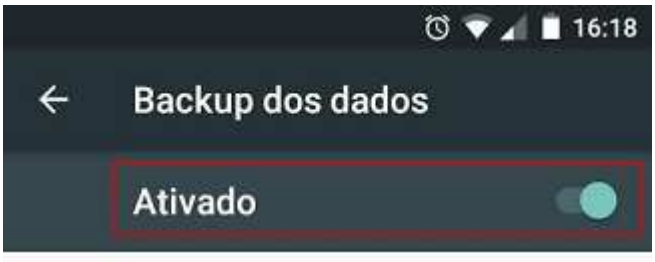

Figura 1.3: O controle de ativação do backup, destacado em vermelho

Capítulo 2

Interface do Usuário

Este capítulo concentra recomendações de segurança que dizem respeito à interface do usuário. Como mencionado no prefácio, estas recomendações possuem como características, serem práticas e prudentes, fornecerem um claro benefício em relação à segurança, e gerarem um impacto mínimo na usabilidade do dispositivo Android.

2.1 Atualizar o dispositivo para a versão mais recente do Android

Seguir esta recomendação garante que a versão do sistema operacional Android instalada no dispositivo seja sempre a mais recente. As versões atualizadas geralmente trazem consigo correções para falhas críticas de segurança.

Assim, manter o sistema Android sempre atualizado reduz a probabilidade de pessoas mal intencionadas e com competência técnica, explorarem remotamente vulnerabilidades presentes no dispositivo.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Sistema
4. Pressionar Sobre o telefone
5. Pressionar Atualizações do Sistema

Vale lembrar que, dependendo do modelo e do fabricante do dispositivo Android, atualizações do sistema podem não estar disponíveis. Para se resguardar dessa possibilidade, recomenda-se:

- verificar se o dispositivo possui uma agenda de atualizações no site do fabricante e/ou em sites especializados, antes de adquiri-lo
- o site do fabricante e outros sites especializados também constituem uma fonte de consulta válida, caso o dispositivo já tenha sido adquirido
- contactar a operadora de telefonia também pode ser uma opção, para obter detalhes sobre a atualização do sistema Android

2.2 Habilitar o bloqueio do dispositivo através de senha

Esta recomendação determina que uma senha seja sempre solicitada antes de se permitir o acesso ao dispositivo. É altamente recomendado que uma senha seja configurada. Obviamente, a falta de uma senha diminui o esforço para acessar os dados armazenados no dispositivo.

1. Pressionar Configurar
2. Deslizar até seção Pessoais
3. Pressionar Segurança
4. Pressionar Bloqueio de Tela
5. Pressionar Senha
6. Digitar uma senha, e pressionar Próximo, para confirmá-la.
7. Confirmar a senha, e pressionar Próximo

2.3 Configurar o modo de espera da tela

Esta recomendação define a quantidade de minutos em que o dispositivo pode ficar inativo antes de requerer a senha novamente. Claro que, quanto menor o tempo, menor será a probabilidade de pessoas mal intencionadas acessarem informações sem a necessidade de se digitar uma senha. O tempo recomendado é de no máximo, dois minutos.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Dispositivo
4. Pressionar Tela
5. Pressionar Modo de espera
6. Selecionar a opção 2 minutos, ou um período menor

2.4 Desabilitar o recurso Notificação de Redes

Este é um recurso do sistema Android que orienta o dispositivo a procurar por uma rede Wi-Fi, quando o usuário tenta acessar a internet e ele não se encontra na faixa de uma rede previamente usada. Quando está ativada e uma nova rede encontra-se disponível, um ícone surgirá na barra de status do dispositivo, que por sua vez exibirá uma lista de redes disponíveis.

Qual o problema em manter a notificação de redes ativada? Ela aumenta o risco de o dispositivo conectar-se inadvertidamente a uma rede não confiável. Isso pode ocorrer caso tal rede possua o mesmo nome de uma confiável previamente usada.

1. Pressionar o botão Aplicativos

2. Pressionar Configurar
3. Deslizar até a seção Configurações de redes
4. Pressionar Wi-Fi
5. Exibir o menu de contexto, pressionando ⋮
6. Pressionar Avançado
7. Deslizar controle de Notificação de rede para a posição Desativado

2.5 Desabilitar o Bluetooth

A tecnologia Bluetooth permite a conexão de diversos acessórios ao dispositivo (fones de ouvido, kits veiculares, teclados, e outros) sem a necessidade de fios. É recomendado que tal recurso permaneça desativado quando não estiver em uso, caso contrario haverá um aumento do risco de descoberta do dispositivo e de conexão a serviços desconhecidos e não confiáveis baseados nesta tecnologia.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Configurações de redes
4. Pressionar Bluetooth
5. Deslizar controle de Bluetooth para a posição Desativado

2.6 Apagar as informações armazenadas no dispositivo antes de se desfazer dele

Recomenda-se apagar todas as informações contidas no armazenamento interno do dispositivo, restaurando-o para as configurações padrões de fábrica, antes de se desfazer do dispositivo. Algumas possíveis situações, são:

- entregar o aparelho para a assistência técnica, para conserto
- vendê-lo para outra pessoa
- doá-lo a alguém
- jogá-lo diretamente no lixo

Manter informações pessoais no dispositivo antes de repassá-lo, aumenta o risco de pessoas maliciosas acessarem e publicarem informações confidenciais previamente armazenadas. Esta tem sido uma das principais causas de muitos vazamentos de fotos e vídeos íntimos na internet.

Por fim, recomenda-se a realização de cópias de segurança (backups) das informações mais importantes, antes de se realizar a remoção das informações.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Fazer backup e redefinir
5. Pressionar Restaurar dados de fábrica
6. Pressionar RESTAURAR TELEFONE
7. Digitar a senha, caso seja necessário
8. Pressionar Próximo
9. Pressionar Restaurar

2.7 Bloquear o cartão SIM

O cartão SIM, conhecido como chip da operadora de telefonia celular, permite a realização de ligações telefônicas, além do armazenamento de informações de contatos, e de outras informações pessoais. Esta recomendação faz com que o dispositivo solicite um PIN (número pessoal de identificação) para que o conteúdo armazenado no chip possa ser acessado. Do contrário, outras pessoas, além do proprietário do chip, poderão acessar seu conteúdo, bem como utilizá-lo em outros dispositivos.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Segurança
5. Pressionar Configurar bloqueio do SIM
6. Pressionar Bloquear cartão SIM
7. Pressionar OK, entendi
8. Digitar o PIN antigo
9. Pressionar OK.
10. Digitar o novo PIN do cartão SIM
11. Pressionar OK
12. Redigitar o novo PIN do cartão SIM
13. Pressionar OK

Duas ressalvas a respeito dessa recomendação. Primeiro, o chip possui um PIN padrão da operadora de telefonia. Segundo, digitar várias vezes incorretamente o PIN, bloqueará o chip. Para habilitá-lo novamente, obtenha o PUK, que é o código de desbloqueio do PIN. Tanto o PIN padrão quanto o PUK constam do manual do chip, quando o mesmo é adquirido na operadora da telefonia celular.

2.8 Desabilitar a visualização de senhas

Esta configuração faz com que as senhas do usuário não sejam exibidas, à medida em que elas são digitadas no dispositivo. A justificativa é que sempre existe a possibilidade de uma pessoa mal intencionada observar a senha que está sendo digitada, ou fragmentos dela, podendo assim adivinhar o restante da senha.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Segurança
5. Deslizar controle de Tornar as senhas visíveis c

2.9 Criptografar o dispositivo

Dispositivos móveis em geral contêm senhas e outras credenciais que habilitam pessoas mal intencionadas a recuperarem informações confidenciais de outros recursos com os quais o dispositivo interage. Criptografar todo o conteúdo do dispositivo diminuirá tal ameaça. Do contrário, informações confidenciais armazenadas no dispositivo poderão ser facilmente obtidas, através de uma grande variedade de métodos.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Segurança
5. Pressionar Codificar telefone, ou Codificar tablet
6. Ler atentamente as instruções e reassalvas exibidas pelo dispositivo
7. Caso o usuário queira continuar com a codificação, pressionar CODIFICAR TELEFONE, ou CODIFICAR TABLET
8. Pressionar Continuar
9. Pressionar novamente Codificar dispositivo, ou Codificar tablet

Há duas ressalvas. Primeiro, o processo é demorado, requer que o dispositivo esteja com a bateria completamente carregada, e permaneça ligado na tomada. Caso o processo seja interrompido, informações poderão ser perdidas. E segundo, uma vez que o processo termine, o dispositivo exigirá um PIN ou uma senha previamente configurada, sempre que o mesmo for ligado.

2.10 Desabilitar a instalação de aplicativos a partir de fontes desconhecidas

Esta recomendação sugere que aplicativos sejam instalados apenas a partir da loja oficial do Google, a Google Play. Instalar aplicativos a partir de diferentes sites e outras alternativas não confiáveis, aumenta o risco de instalação (inadvertida ou não) de aplicativos maliciosos.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Segurança
5. Na seção Administração do dispositivo, deslizar o controle de Fontes desconhecidas para a posição desativado

Capítulo 3

Configurações avançadas

Este capítulo também concentra recomendações de segurança que dizem respeito à interface do usuário. Porém, devido às suas características peculiares, destinam-se a dispositivos Android nos quais a segurança é primordial. Estas recomendações podem impactar significamente a usabilidade do dispositivo Android, por isso é recomendado considerá-las como medidas de defesa em profundidade.

3.1 Criar uma senha alfanumérica

Esta recomendação apenas sugere que o leitor crie uma senha composta não de números, de letras, e símbolos especiais para desbloquear a tela do dispositivo Android.

Esta Configurar é bem simples. Basta tomar este cuidado ao criar ou alterar uma senha, no passo 8 da seção 2.2.

A digitação frequente de uma senha mais complexa será, com certeza, tediosa e complicada. Por isso, será necessário ponderar entre o nível de segurança desejado e a frequência de uso do dispositivo, antes da criação da senha.

3.2 Desabilitar a depuração via USB

A depuração via USB é extremamente útil... Para os desenvolvedores de aplicativos Android. Ela permite que os desenvolvedores alterem o comportamento padrão do dispositivo, enviem comandos para o mesmo, e acessem as informações armazenadas.

É recomendável desabilitar este recurso, pois na maioria dos dispositivos Android, a mesma entrada física usada para acessar informações, é usada também para recarregar a bateria. Assim, manter habilitadas as funções de dados e de comandos, aumenta a probabilidade de ataque ao dispositivo.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Sistema
4. Pressionar Programador
5. Desmarcar a caixa Depuração USB

6. Na sub-seção Depuração, desmarcar a caixa Depuração USB

A opção Programador só será visível se o usuário habilitar explicitamente os recursos de desenvolvimento. Isso é feito pressionando o número da versão do Android sete vezes seguidas. Caso o usuário não tenha interesse no desenvolvimento de aplicativos para Android, convém não habilitar os recursos de desenvolvimento.

3.3 Remover as redes Wi-Fi já acessadas

Esta recomendação faz com que o dispositivo Android esqueça redes Wi-Fi que já foram acessadas pelo usuário.

Uma rede Wi-Fi confiável sempre será passível de fraude, e sempre existirá o risco de dispositivo se conectar a ela caso o usuário a mantenha cadastrada. Além disso, caso esta rede possua um nome padrão (como "default" ou "D-Link" por exemplo), a probabilidade de que o dispositivo conecte-se a ela automaticamente aumenta ainda mais.

1. Pressionar o botão Aplicativos
2. Pressionar Wi-Fi
3. Exibir o menu de contexto, pressionando ⋮
4. Selecionar Redes salvas
5. Pressionar as redes a serem esquecidas e logo após, pressionar Esquecer

3.4 Desabilitar todo o recurso de redes Wi-Fi

Em ambientes onde a segurança é prioridade, recomenda-se que o recurso de conexão a redes Wi-Fi permaneça desabilitado no dispositivo Android. Caso ele possua acesso a serviços de dados celulares (3G ou 4G por exemplo), a conexão à internet deverá ocorrer através destas redes.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Pressionar Wi-Fi
4. Desativar o recurso Wi-Fi

3.5 Desabilitar o serviço de localização

O serviço de localização permite que alguns aplicativos instalados no dispositivo obtenham e usem informações que indiquem a localização física do usuário. Esta localização é determinada através do GPS do dispositivo, da rede celular 3G ou 4G, e de redes Wi-Fi. Se o usuário desativar os serviços de localização, ele receberá do solicitações para reativá-la, sempre que algum aplicativo quiser fazer uso deste recurso.

Manter o serviço de localização ativado aumenta a capacidade de pessoas mal intencionadas, com considerável conhecimento técnico, rastrearem a localização do usuário através de sites web, aplicativos, etc.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Localização
5. Desativar o serviço de localização

3.6 Habilitar o Modo Avião

Quando está habilitado, o Modo Avião desativa todos os transmissores e receptores de sinais de rádio do dispositivo. Alguns serviços desativados, são:

- Envio e recebimento de ligações
- Envio e recebimento de SMS e MMS
- Dados móveis (3G, 4G)
- GPS
- Wi-Fi
- Bluetooth

Assim, quando estas funcionalidades forem desnecessárias, é recomendado manter o dispositivo no Modo Avião. Caso a transmissão e recepção de sinais permaneçam habilitados mesmo sem necessidade, haverá um aumento da possibilidade de que estes sinais de rádio sejam usados como um meio para se atacar remotamente o dispositivo.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Na seção Redes, pressionar Mais
4. Pressionar Modo avião

3.7 Desabilitar a exibição de notificações

Esta recomendação determina que absolutamente nenhuma notificação seja exibida na tela do dispositivo, quando a mesma encontrar-se bloqueada.

Assim, caso o dispositivo seja perdido, roubado ou furtado, pessoas com interesses maliciosos não poderão obter informações confidenciais a partir das notificações exibidas na tela bloqueada do dispositivo.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Dispositivo
4. Pressionar Som e notificação
5. Na seção Notificação, pressionar Com o dispositivo bloqueado
6. Pressionar a opção Não mostrar notificações

3.8 Limitar a quantidade de mensagens SMS e MMS

Esta configuração determina a quantidade de mensagens, por conversa, que devem permanecer armazenadas no dispositivo. Quando o limite configurado é atingido, as mensagens mais antigas serão apagadas, caso o dispositivo esteja devidamente configurado.

Caso o dispositivo seja comprometido de alguma forma, o impacto do vazamento de informação, será menor, caso a quantidade de mensagens armazenadas seja pequena.

1. Pressionar o ícone Mensagens
2. Exibir o menu de contexto, pressionando ⋮
3. Pressionar Configurações
4. Marcar a caixa Excluir mensagens antigas
5. Para configurar o limite de SMS, executar os seguintes passos:
   (a) Pressionar Limite de mensagens de texto
   (b) Digitar o limite de 100 mensagens
   (c) Pressionar Definir
6. E para configurar o limite de MMS, executar os seguintes passos:
   (a) Pressionar Limite de mensagens multimidia
   (b) Digitar o limite de 60 mensagens
   (c) Pressionar Definir

3.9 Habilitar o Android Device Manager

Esta recomendação, se seguida, facilitará a busca e a recuperação de dispositivos Android roubados, furtados, ou perdidos.

Existem vários aplicativos na Play Store, com funcionalidade similar. Aqui, é dada preferência ao Android Device Manager, que é uma solução nativa da plataforma Android.

Cabe aqui um aviso importante. Em caso de roubo ou furto, recomenda-se que o usuário não tente recuperar o dispositivo sozinho, mas sim com o auxílio da força policial.

Mais um aviso. Para que o Android Device Manager seja o mais efetivo possível, será necessário que os recursos de dados móveis (3G, e 4G), Wi-Fi, e os serviços de localização, permaneçam sempre habilitados, e este pré-requisito contradiz algumas recomendações anteriores. Porém, não habilitar o recurso diminuirá significativamente a possibilidade de se recuperar o dispositivo. Assim, cabe ao usuário ponderar sobre quais recomendações são mais importantes para ele.

1. Pressionar o botão Aplicativos
2. Pressionar Configurar
3. Deslizar até a seção Pessoais
4. Pressionar Segurança
5. Na secao Administração do dispositivo, pressionar Selecionar administradores
6. Marcar a caixa Gerenciador de dispositivos Android

Quando o Android Device Manager está configurado, pode-se gerenciar o dispositivo remotamente de duas formas, em caso de perda, roubo, ou furto:

- acessando o endereço https://www.google.com/android/devicemanager
- instalando o aplicativo Android Device Manager em algum outro dispositivo Android

Capítulo 4

Configurações para o navegador Chrome

Este capítulo traz recomendações de segurança que dizem respeito ao Google Chrome, que é o navegador web padrão do sistema Android 6.0.

Analogamente às recomendações do capítulo anterior, elas impactam significamente a usabilidade do Chrome. Por isso é recomendado considerá-las como medidas de defesa em profundidade e destiná-las apenas a dispositivos Android nos quais a segurança é primordial.

4.1 Desabilitar a execução de código Javascript

JavaScript é uma linguagem de programação originalmente implementada como parte dos navegadores web para que scripts possam ser executados do lado do cliente e interajam com o usuário, controlando o navegador, e alterando o conteúdo da página exibida.

É recomendado que a linguagem Javascript não tenha permissões de execução no navegador do dispositivo, pois ela pode ser sua utilizada como vetor de diversos tipos de ataques aos usuários do navegador Chrome. Alguns exemplos de ataques são:

- exibição de páginas web maliciosas, através de janelas pop-ups
- manipulação de credenciais de login

Por outro lado, a grande maioria dos sites web faz uso da tecnologia Javascript para permitir uma maior interatividade. Assim, desabilitando a execução de código Javascript, a experiência do usuário ficará bastante reduzida.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Configurações do site
5. Pressionar Javascript
6. Desativar o Javascript, deslizando o controle para a esquerda

4.2 Desativar o preenchimento automático de formulários

O Chrome permite que informações digitadas em formulários de sites web sejam armazenadas para que, em outras visitas aos mesmos sites, essas mesmas informações possam ser preenchidas automaticamente.

Porém, para fins de segurança, é recomendado que este recurso seja desabilitado, do contrário aumentará a probabilidade de pessoas mal intenciondas tecnicamente qualificadas obterem ou usarem informações confidenciais armazenadas no dispositivo, tais como:

- nomes
- números de cartões de crédito
- senhas

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Preenchimento automático de formulários
5. Desativar o Preenchimento automático de formulários

4.3 Desativar a aceitação de Cookies

Cookies HTTP são pequenos arquivos texto enviados de sites web e armazenados no navegador Chrome. Estes arquivos podem, eventualmente, conter informações importantes a respeito do usuário, como logins, senhas, e números de contas bancárias.

Ao configurar o navegador do dispositivo para não aceitar e nem armazenar cookies HTTP, a probabilidade de pessoas tecnicamente habilitadas rastrearem, adulterarem, ou roubarem informações confidenciais diminuirá bastante.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Configurações do site
5. Pressionar Cookies
6. Desativar o uso de Cookies, deslizando o controle para a esquerda

4.4 Habilitar o recurso de Navegação segura

Seguindo esta recomendação, o Chrome protegerá tentara proteger o usuario de certos tipos de ataques, malware, e sites de phishing.

Manter este recurso desabilitado aumenta a exposição do usuário a diversos tipos de ataques que podem comprometer suas informações pessoais.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Privacidade
5. Marcar a opção Navegação segura

4.5 Bloquear a exibição de janelas pop-up

O bloqueador de janelas pop-up é usado para bloquear as janelas que um site web pode abrir, com ou sem o consentimento do usuário.

A razão para desabilitar tal recurso é que janelas pop-up têm sido usadas por pessoas mal intencionadas e com conhecimento técnico, para distribuir conteúdo não confiável e malicioso entre os usuários, sem que estes percebam.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Configurações do site
5. Bloquear as janelas pop-up, deslizando o controle para a esquerda

4.6 Desabilitar o armazenamento de senhas

Este recurso permite que senhas digitadas em websites sejam armazenadas no Chrome. Em visitas subsequentes aos mesmos websites, essas senhas são preenchidas automaticamente.

Porém, para fins de segurança, é fortemente recomendado que este recurso seja desabilitado. Caso uma pessoa mal intencionada obtenha acesso ao dispositivo, ela poderá usar as senhas armazenadas.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Salvar senhas
5. Desativar o salvamento de senhas, deslizando o controle para a esquerda

4.7 Desabilitar o Serviço de localização

O serviço de localização permite que websites obtenham e usem a localização física do usuário. Tal localização é determinada através de rede celular, de redes Wi-Fi próximas, e claro, do GPS.

Caso o usuário desative o serviço de localização, o dispositivo solicitará ao usuário a reativação, sempre que algum website necessitar.

Manter o serviço de localização ativado, aumenta a capacidade de uma pessoa mal intencionada determinar ou rastrear a localização do usuário através de sites web, aplicativos instalados localmente, ou outros meios.

1. Pressionar o ícone do navegador Chrome
2. Pressionar o botão de configuração, o canto superior direito do navegador (⋮)
3. Pressionar Configurações
4. Pressionar Configurações do site
5. Desativar a localização, deslizando o controle para a esquerda

Parte II

Apple iOS 10

Capítulo 5

Introdução

Este capítulo tem o objetivo de definir algumas premissas básicas, antes de se iniciar com as recomendações de segurança. A primeira delas é que o sistema operacional iOS pode ser encontrado em uma gama diversa de aparelhos, como iPhones, iPads, e o iPod Touch. Por isso, com o objetivo de simplificar a nomenclatura utilizada, tais equipamentos serão referenciados daqui por diante como dispositivos iOS.

Todas as recomendações aqui descritas foram testadas em um iPad de quarta geração e em um iPhone 5s. As instruções das recomendações de segurança foram criadas com base na interface de usuário destes dispositivos. No caso deles, todas recomendações listadas quase sempre têm início pressionando o botão Ajustes. Segue abaixo a localização deste botão.

Figura 5.1: O botão Ajustes, destacado em vermelho

É necessário enfatizar que estas recomendações tratam da versão 10.0 do iOS. O leitor pode verificar se esta é a versão presente em seu dispositivo seguindo as instruções logo abaixo.

1. Pressionar o botão Ajustes
2. Pressionar Geral
3. Pressionar Sobre
4. Verificar se o valor de Versão é 10 ou superior

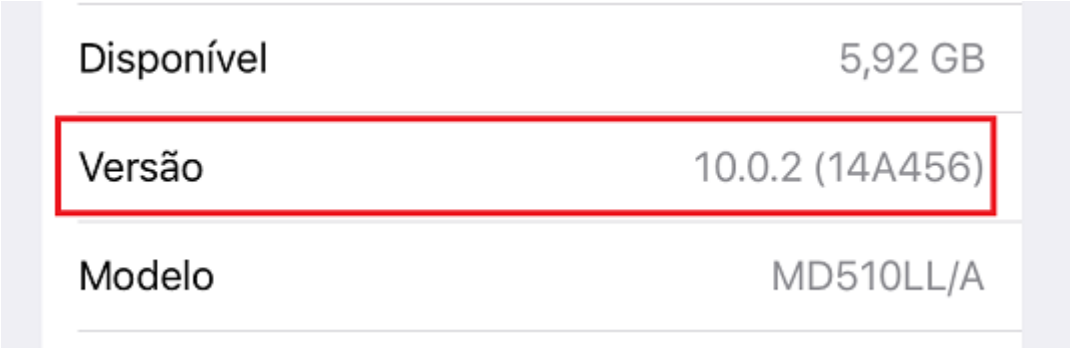

Figura 5.2: A versão presente no dispositivo usado para testes, destacada em vermelho

Vale lembrar que o autor não se responsabiliza por eventuais danos causados em dispositivos iOS decorrentes da aplicação das configurações recomendadas aqui. Por isso, é sugerido que, se possível, estas recomendações sejam aplicadas inicialmente em aparelhos de teste para, apenas depois, serem aplicadas em outros dispositivos.

Realizar backups das informações contidas no dispositivo também é uma prática recomendável para a recuperação de informações importantes, caso ocorram eventuais problemas.

Seguem logo abaixo instruções para a realização de backups em dispositivos iOS:

1. Pressionar o botão Ajustes
2. Pressionar iCloud
3. Selecionar para backup todas as informações que o usuário considerar importantes (E-mail, Contatos, etc.)
4. Pressionar Backup
5. Na tela seguinte, ativar Backup do iCloud deslizando o controle para a direita
6. Na mesma tela, caso o usuário esteja conectado a uma rede Wi-Fi, pressionar Efetuar Backup Agora

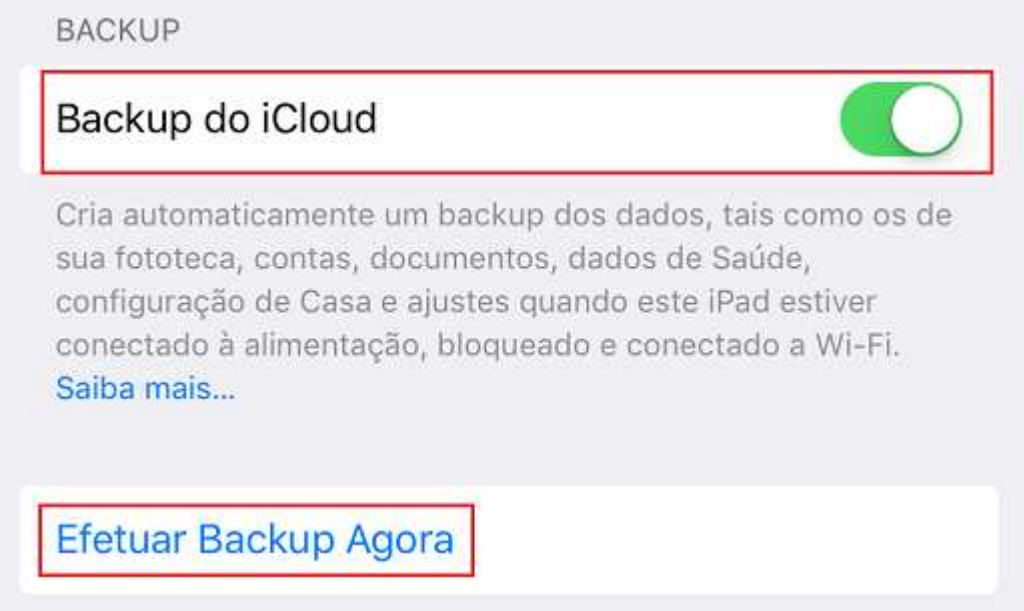

Figura 5.3: Os controles de habilitação e realização de backups, ambos destacados em vermelho

Capítulo 6

Interface do Usuário

Este capítulo concentra recomendações de segurança que dizem respeito à interface do usuário. Como mencionado no prefácio, estas recomendações possuem como características, serem práticas e prudentes, fornecerem um claro benefício em relação à segurança, e gerarem um impacto mínimo na usabilidade do dispositivo iOS.

6.1 Atualizar o dispositivo para a versão mais recente do iOS

Seguir esta recomendação garante que a versão do sistema operacional iOS instalada no dispositivo seja sempre a mais recente. As versões atualizadas geralmente trazem consigo correções para falhas críticas de segurança.

Assim, manter o sistema iOS sempre atualizado reduz a probabilidade de pessoas mal intencionadas e com competência técnica, explorarem remotamente vulnerabilidades presentes no dispositivo.

Há duas maneiras de se verificar atualizações do iOS estão disponíveis. Via OTA (over-the-air), ou através do iTunes. Caso o leitor queira verificar atualizações via OTA, deve-se fazer o seguinte:

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Atualização de Software
4. Caso alguma atualização esteja disponível, pressionar Download
5. Após o download, pressionar Instalar, para atualizar o iOS

Caso o leitor queira verificar atualizações através do iTunes, deve-se fazer o seguinte:

1. Conectar o dispositivo ao computador
2. Abrir o iTunes
3. Na lista de dispositivos, selecionar o dispositivo a ser atualizado
4. Clicar em Verificar Atualizações

5. Caso haja alguma atualização disponível, clicar em Baixar e Instalar

É bom lembrar que não se deve desligar nem desconectar o dispositivo (no caso da atualização via iTunes) enquanto o processo de atualização não terminar!

6.2 Remover aplicativos que não serão utilizados

Uma novidade trazida pelo iOS 10 em relação às suas versões anteriores é a possibilidade de se remover aqueles aplicativos pré-instalados (ou de fábrica). É deste tipo de aplicativo que trata esta recomendação. Seguem logo abaixo as instruções para se realizar a remoção de tais aplicativos:

1. Na tela desbloqueada, localizar o ícone do aplicativo que se deseja remover
2. Pressionar e "segurar" o ícone do aplicativo em questão
3. Pressionar o pequeno X, no canto superior esquerdo do ícone
4. Confirmar a remoção do aplicativo
5. Repetir este procedimento para quaisquer outros aplicativos que se deseje remover

É preciso notar que nem todos os aplicativos instalados de fábrica pode ser removidos. Isso se deve ao fato de que eles fazem parte do sistema operacional iOS, e por isso não podem ser descartados.

Algumas brechas de segurança em dispositivos móveis são o resultado de falhas ou problemas com os aplicativos instalados. Por isso, diminuir a quantidade de aplicativos instalados no dispositivo diminuirá as chances de que pessoas mal-intencionadas possam usar tais falhas para invadir ou tomar o controle do dipositivo.

6.3 Habilitar o bloqueio do dispositivo através de código

Esta recomendação determina que um código de bloqueio seja sempre solicitado antes de se permitir o acesso ao dispositivo.

É altamente recomendado que um código de bloqueio seja configurado, para que pessoas estranhas não adquiram acesso fácil e imediato às informações armazenadas no dispositivo.

1. Pressionar Ajustes
2. Pressionar Código ou Touch ID e Código
3. Pressionar Ativar Código
4. Digitar um código
5. Digitar novamente o código

6.4 Desabilitar os widgets na tela de bloqueio

Segundo a definição da própria Apple, um widget é uma extensão que exibe uma pequena quantidade de informação util e periódica, ou uma funcionalidade específica de um aplicativo.

Tais widgets podem ser acessados por padrão na tela de bloqueio, o que pode representar uma verdadeira ameaça à privacidade do usuário. Aqui estão as instruções para desabilitá-la inteiramente.

1. Pressionar Ajustes
2. Pressionar Código ou Touch ID e Código
3. Na seção Permitir Acesso Quando Bloqueado, desabilitar o controle Visualização para Hoje
4. Desabilitar também a Visualização de Notificações

Caso alguma informação exibida por algum widget seja considerada confidencial ou sensível, tem-se aí um grande risco de vazamento de dados, já que manter os widgets acessíveis na tela de bloqueio permitirá que qualquer pessoa com acesso físico ao dispositivo iOS visualize informações exibidas por eles.

É importante notar que após esta configuração, os widgets continuarão acessíveis ao usuário, uma vez que ele desbloqueie o dispositivo.

6.5 Desinstalar aplicativos de fábrica que náo serão utilizados

Uma outra novidade trazida pelo iOS 10, foi a possibilidade de se remover os aplicativos instalados de fábrica. Segue abaixo

6.6 Configurar o modo de espera da tela

Esta recomendação define a quantidade de minutos em que o dispositivo pode ficar inativo antes de requerer a senha novamente. Claro que, quanto menor o tempo, menor será a probabilidade de pessoas mal intencionadas acessarem informações sem a necessidade de se digitar uma senha. O tempo recomendado é de dois minutos.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Bloqueio automático
4. Selecionar 2 minutos

6.7 Desativar o recurso de VPN

Dispositivos iOS podem se conectar nativamente a serviços de VPN que usam os seguintes protocolos:

- L2TP sobre IPSec
- PPTP
- IPSec da Cisco

Caso o dispositivo possua uma conexão VPN configurada, ele só deve ser ativado quando for necessário. Do contrário, aplicativos maliciosos ou "trojanizados", podem acessar os recursos de VPN do dispositivo.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar VPN
4. Desativar o recurso de VPN, caso ele esteja ativado

6.8 Desativar o Bluetooth

A tecnologia Bluetooth permite a conexão de diversos acessórios ao dispositivo (fones de ouvido, kits veiculares, teclados, e outros) sem a necessidade de fios.

É recomendado que tal recurso permaneça desativado quando não estiver em uso, caso contrário haverá um aumento do risco de descoberta do dispositivo e de conexão a serviços desconhecidos e não confiáveis baseados nesta tecnologia.

1. Pressionar Ajustes
2. Pressionar Bluetooth
3. Desativar o Bluetooth, caso ele se encontre ativado

6.9 Desativar o AirDrop

Esta configuração evita que o dispositivo seja descoberto, via Airdrop, por alguém (incluindo os contatos).

A justificativa para a sua desativação é a mesma do caso do Bluetooth, na seção anterior.

1. Desbloquear o dispositivo
2. Deslizar a parte inferior da tela para cima, a fim de exibir a Central de Controle
3. Pressionar o campo AirDrop na parte inferior da Central de Controle
4. Pressionar Inativo

6.10 Desativar as solicitações de conexão a redes Wi-Fi

Quando o dipositivo (seja ele um iPhone, um iPad, ou um iPod) tenta se conectar à internet mas não está em uma faixa de redes Wi-Fi previamente utilizada, ele procura por outras redes e exibe uma lista de todas as redes Wi-Fi disponíveis, para que o usuário escolha alguma.

É recomendado que tal funcionalidade seja desativada. O usuário terá de configurar e se conectar manualmente a uma rede Wi-Fi, mas este comportamento reduz as chances de se conectar inadvertidamente a redes não confiáveis.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Desativar a opção Solicitar Conexão

6.11 Habilitar o download automático de atualizações de aplicativos

Esta recomendação garante que as versões dos aplicativos instalados no dispositivo sejam sempre as mais recentes.

A justificativa é que as versões mais recentes geralmente trazem consigo correções para falhas críticas de segurança.

1. Pressionar Ajustes
2. Pressionar iTunes Store e App Store
3. Na seção TRANSFERÊNCIAS AUTOMÁTICAS, ativar a opção Atualizações

6.12 Apagar as informações armazenadas no dispositivo antes de se desfazer dele

Recomenda-se apagar todas as informações contidas no armazenamento interno do dispositivo, restaurando-o para as configurações padrões de fábrica, antes de se desfazer dele.

Algumas situações incluem:

- entregar o aparelho para a assistência técnica, para conserto
- vendê-lo para outra pessoa
- doá-lo a alguém
- jogá-lo diretamente no lixo

Manter informações pessoais no dispositivo antes de repassá-lo, aumenta o risco de pessoas maliciosas acessarem e publicarem informações confidenciais armazenadas. Esta tem sido uma das principais causas de vazamentos de fotos e vídeos íntimos na internet.

Realizar cópias de segurança (backups) das informações, antes de se realizar a remoção das mesmas, tambem é importante.

Antes de se restaurar o dispositivo para as configurações de fábrica, é necessário desativar o serviço iMessage, procedendo da seguinte forma:

1. Pressionar Ajustes
2. Pressionar Mensagens
3. Desativar o iMessage

E finalmente, seguem logo abaixo as instruções para se restaurar o dispositivo, apagando quaisquer informações pessoais armazenadas:

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Redefinir
4. Pressionar Redefinir Todos os Ajustes
5. Digitar o código, caso o mesmo tenha sido previamente configurado

Capítulo 7

Configurações avançadas

Este capítulo também concentra recomendações de segurança que dizem respeito à interface do usuário. Porém, devido às suas características peculiares, destinam-se a dispositivos iOS nos quais a segurança é primordial. Estas recomendações podem impactar significamente a usabilidade do dispositivo, por isso é recomendado considerá-las como medidas de defesa em profundidade.

7.1 Desabilitar o uso de códigos de desbloqueio simples

Esta recomendação determina que códigos de bloqueio de apenas quatro dígitos não sejam permitidos para se proteger o acesso ao dispositivo. É recomendado que o dispositivo seja configurado para permitir o uso de códigos de bloqueio com mais de quatro caracteres alfanúmericos (números, letras, símbolos, etc).

Permitir uma senha alfanumérica para desbloquear o dispositivo iOS aumenta a dificuldade que uma pessoa mal intencionada terá na tentativa de realizar acessos não autorizados.

1. Pressionar Ajustes
2. Pressionar Código, ou Touch ID e Código
3. Pressionar Alterar Código, ou Ativar Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Pressionar Opções de código
6. Pressionar Código Alfanumérico Personalizado
7. Digitar um código alfanumérico e pressionar Seguinte
8. Digitar novamente o código alfanumérico e pressionar OK

7.2 Habilitar a eliminação de informações

Esta configuração determina que o dispositivo iOS apague todo o seu conteúdo (vídeos, fotos, etc) após dez tentativas fracassadas de desbloqueio.

Sucessivas tentativas fracassadas de desbloqueio do aparelho sugerem que ele não se encontra nas mãos de seu proprietário. Neste caso, apagar todo o conteúdo garante a confidencialidade das informações armazenadas no dispositivo.

1. Pressionar Ajustes
2. Pressionar Código, ou Touch ID e Código
3. Pressionar Alterar Código, ou Ativar Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Ativar a opção Eliminar Dados

7.3 Desativar o desbloqueio através do Touch ID

O Touch ID permite o uso de uma ou mais impressões digitais como código de desbloqueio, através de um simples toque do botão Home. O sensor do Touch ID "lê" a impressão digital e automaticamente desbloqueia o telefone.

Desabilitar este recurso evita o risco de uma autenticação não autorizada via Touch ID, seja através de falsos positivos, seja através de ataques intencionais.

1. Pressionar Ajustes
2. Pressionar Geral
3. Pressionar Código, ou Touch ID e Código
4. Caso algum código já tenha sido configurado, será necessário digitá-lo
5. Desativar a opção Desbloquear iPhone, ou Desbloquear iPad

Vale lembrar que esta configuração se aplica apenas a dispositivos iOS mais recentes.

7.4 Desabilitar o acesso à Central de Controle a partir da tela bloqueada

Ao longo da história do sistema iOS, já foram descobertas algumas maneiras de se contornar a proteção da tela bloqueada. Esta recomendação desabilita o acesso à Central de Controle a partir da tela.

A ideia aqui é eliminar a possibilidade de a Central de Controle vir ser usada como um meio para se contornar a proteção da tela bloqueada.

1. Pressionar Ajustes
2. Pressionar Central de Controle
3. Desativar a opção Acesso na Tela Bloqueada

7.5 "Esquecer" redes Wi-Fi

Esta configuração faz com que o dispositivo iOS "esqueça" redes Wi-Fi nas quais ele já tenha conectado.

Uma rede Wi-Fi confiável, mas sem autenticação, pode ser mascarada e o dispositivo pode se conectar automaticamente a ela se a mesma não tiver sido "esquecida" pelo dispositivo desde a última conexão.

Outra situação possível é quando a rede Wi-Fi mantém seu nome padrão, de fábrica, e o dispositivo iOS encontra uma outra rede não confiável de mesmo nome e acabe tentando se conectar a ela automaticamente.

Para esta recomendação, é necessário que o Wi-Fi esteja ativado e a rede Wi-Fi a ser esquecida esteja próxima ao dispositivo.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Na lista ESCOLHA UMA REDE..., localizar a rede a ser esquecida e pressionar o símbolo de exclamação.
4. Na tela seguinte, pressionar Esquecer Esta Rede
5. Confirmar o esquecimento da rede

7.6 Desabilitar todo o recurso de redes Wi-Fi

Em ambientes onde a segurança é prioridade, recomenda-se que o recurso de conexão a redes Wi-Fi permaneça desabilitado no dispositivo Android. Caso ele possua acesso a serviços de dados celulares (3G ou 4G por exemplo), a conexão à internet deverá ocorrer através destas redes.

1. Pressionar Ajustes
2. Pressionar Wi-Fi
3. Desativar a Wi-Fi

7.7 Desabilitar o Acesso Pessoal

O Acesso Pessoal permite que o usuário compartilhe sua conexão à internet, via 3G ou 4G, com outros dispositivos, através de Wi-Fi, Bluetooth, ou cabo USB.

Desabilitar o Acesso Pessoal, quando o mesmo não é necessário, elimina a possibilidade de o recurso vir a ser usado como um meio para que pessoas mal intencionadas tecnicamente preparadas ataquem remotamente o dispositivo iOS.

1. Pressionar Ajustes
2. Pressionar Acesso Pessoal
3. Desativar o Acesso Pessoal, caso ele se encontre ativado

7.8 Desabilitar o serviço de localização

O serviço de localização permite que alguns aplicativos instalados no dispositivo iOS obtenham e usem informações que indiquem a localização física do usuário. Esta localização é determinada através do GPS do dispositivo, da rede celular 3G ou 4G, e de redes Wi-Fi. Se o usuário desativar os serviços de localização, ele receberá do solicitações para reativá-la, sempre que algum aplicativo quiser fazer uso deste recurso.

Manter o serviço de localização ativado aumenta a capacidade de pessoas mal intencionadas, com considerável conhecimento técnico, rastrearem a localização do usuário através de sites web, aplicativos, etc.

1. Pressionar Ajustes
2. Pressionar Privacidade
3. Pressionar Serv. Localização
4. Na tela seguinte, desativar o serviço de localização

7.9 Habilitar o Modo Avião

Quando está habilitado, o Modo Avião desativa todos os transmissores e receptores de sinais de rádio do dispositivo iOS. Alguns serviços desativados, são:

- Envio e recebimento de ligações
- Envio e recebimento de SMS e MMS
- Dados móveis (3G, 4G)
- GPS
- Wi-Fi
- Bluetooth

Assim, quando estas funcionalidades forem desnecessárias, é recomendado manter o dispositivo no Modo Avião. Caso a transmissão e recepção de sinais permaneçam habilitados mesmo sem necessidade, haverá um aumento da possibilidade de que estes sinais de rádio sejam usados como um meio para se atacar remotamente o dispositivo.

1. Pressionar Ajustes
2. Ativar o Modo avião

7.10 Não exibir notificações de aplicativos na tela bloqueada

Esta configuração previne que notificações oriundas de aplicativos instalados sejam exibidas quando o dispositivo iOS encontra-se bloqueado.

É recomendado que tal visualização seja desabilitada para todos os aplicativos nos quais é desejada confidencialidade. Do contrário, pessoas que não possuem o código de desbloqueio poderão visualizar notificações, aumentando assim o risco de vazamento de informações importantes.

1. Pressionar Ajustes
2. Pressionar Notificações
3. Na lista ESTILO DA NOTIFICAÇÃO, localizar o aplicativo e pressioná-lo
4. Na tela seguinte, desativar a opção Mostrar na Tela Bloqueada
5. Repetir os passos 3 e 4 para outros aplicativos

7.11 Habilitar o recurso Buscar iPhone (ou Buscar iPad)

Esta configuração habilita as seguintes funcionalidades no dispositivo iOS:

- o rastreamento remoto da localização do dispositivo
- a eliminação remota de informações armazenadas no dispositivo
- a exibição remota de mensagens

Habilitar o recurso Buscar iPhone (ou Buscar iPad) no iOS ativa a capacidade de se localizar o dispositivo através do aplicativo iOS Buscar iPhone, ou através do site do iCloud. Também exibe uma mensagem personalizada com um número de telefone à sua escolha na tela bloqueada, e previne a execução de ações importantes sem a digitação da senha do Apple ID, como a eliminação das informações armazenadas no dispositivo iOS e sua configuração.

1. Pressionar Ajustes
2. Pressionar iCloud
3. Pressionar Buscar iPhone (ou Buscar iPad)
4. Na tela seguinte, ativar a opção Buscar iPhone (ou Buscar iPad)

7.12 Habilitar uma senha para acesso ao cartão SIM

O cartão SIM, conhecido como chip da operadora de telefonia celular, permite a realização de ligações telefônicas, além do armazenamento de informações de contatos, e de outras informações pessoais. Este controle assegura que o cartão SIM, caso seja perdido ou roubado, não será usado em nenhum outro dispositivo.

Uma pessoa com intenções maliciosas pode retirar o cartão SIM de um telefone e inseri-lo em outro telefone, realizar ligações, enviar mensagens, etc. Adicionar uma senha ao cartão protegerá contra este tipo de ataque. Tal senha será requisitada pelo dispositivo sempre que o cartão SIM for acessado.

1. Pressionar Ajustes
2. Pressionar Telefone
3. Pressionar PIN do SIM
4. Digitar um PIN

Capítulo 8

Configurações para o navegador Safari

Este capítulo traz recomendações de segurança que dizem respeito ao Safari, que é o navegador web padrão do sistema iOS.

Analogamente às recomendações do capítulo anterior, elas impactam significamente a usabilidade do Safari. Por isso é recomendado considerá-las como medidas de defesa em profundidade e destiná-las apenas a dispositivos iOS nos quais a segurança é primordial.

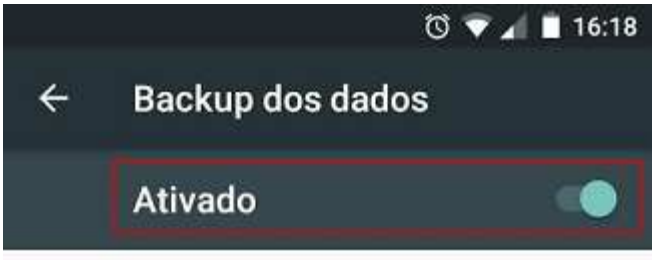

Figura 8.1: A localização padrão do ícone do navegador Safari, destacada em vermelho

8.1 Desabilitar a execução de código Javascript

Javascript tecnologia permite que desenvolvedores de websites controlem certos elementos de páginas web, como exibir a data e hora corrente, ou exibir janelas pop-up.

Neste item, é recomendado que a linguagem Javascript não tenha permissões de execução no navegador web padrão do dispositivo, pois a mesma pode vir a ser utilizada como meio para diversos tipos de ataques aos usuários. Tais ataques vão desde a manipulação de credenciais de login até a exibição de páginas web maliciosas, através de janelas pop-up.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Avançado
4. Desativar Javascript, deslizando controle para a esquerda

8.2 Habilitar o aviso de websites fraudulentos

Este controle habilita o navegador Safari a exibir avisos e impedir o carregamento da páginas de websites potencialmente fraudulentos.

Os avisos podem ajudar a evitar a visitação acidental a algum site de phishing, bem como outros sites desenvolvidos com intenções maliciosas.

1. Pressionar Ajustes
2. Pressionar Safari
3. Na seção PRIVACIDADE E SEGURANÇA, ativar Aviso de Site Fraudulento, deslizando o controle para a direita

8.3 Desabilitar o preenchimento automático de informações de contato

O preenchimento automático configura o navegador Safari a se lembrar de informações comumente digitadas pelo usuário em formulários na internet, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de informações sensíveis ou confidenciais localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Dados de Contato, deslizando o controle para a esquerda

8.4 Desabilitar preenchimento automático de nomes e senhas

O preenchimento automático configura o navegador Safari a se lembrar de credenciais, que geralmente são confidenciais, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de informações sensíveis ou confidenciais localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari

3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Nomes e Senhas, deslizando o controle para a esquerda

8.5 Desabilitar o preenchimento automático de cartões de crédito

O preenchimento automático configura o navegador Safari a se lembrar de números de cartões de crédito, para automatizar o preenchimento de formulários subsequentes.

Desabilitar o preenchimento automático ajuda a evitar o armazenamento de números de cartões de crédito localmente no dispositivo iOS. Também reduz as chances de estas informações serem usadas de maneira não autorizada caso alguma pessoa mal intencionada obtenha acesso ao dispositivo, seja ele um iPhone ou iPad.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Desativar o preenchimento automático para Cartões de Crédito, deslizando o controle para a esquerda

8.6 Apagar informações sobre senhas armazenadas

O navegador Safari fornece um repositório para armazenar informações, incluindo logins e senhas, que por sua vez dão suporte ao recurso de preenchimento automático de formulários. Senhas salvas são armazenadas no "chaveiro" do iCloud ou do dispositivo iOS, seja ele um iPhone ou iPad.

Excluir informações a respeito de credenciais salvas ajuda a impedir o uso delas, em caso de acessos não autorizados ao dispositivo.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Senhas
4. Digitar o código de desbloqueio do dispositivo, caso seja necessário
5. Na tela seguinte, pressionar Editar
6. Pressionar cada credencial exibida, de modo a selecioná-las para remoção
7. Pressionar Apagar
8. Confirmar a remoção das senhas

8.7 Remover informações armazenadas sobre cartões de crédito

O navegador Safari fornece um repositório para armazenar informações, incluindo cartões de crédito, que por sua vez dão suporte ao recurso de preenchimento automático de formulários. Números de cartões de crédito são armazenados no "chaveiro" do iCloud ou do dispositivo iOS, seja ele um iPhone ou iPad.

Excluir informações a respeito de cartões de crédito ajuda a impedir o uso deles, em caso de acessos não autorizados ao dispositivo.

1. Pressionar Ajustes
2. Pressionar Safari
3. Pressionar Preenchimento Automático
4. Pressionar Cartões de Crédito Salvos
5. Digitar o código de desbloqueio do dispositivo, caso seja necessário
6. Na tela seguinte, pressionar Editar
7. Pressionar cada cartão de crédito exibido, de modo a selecioná-los para remoção
8. Pressionar Apagar
9. Confirmar a remoção dos cartões de crédito

8.8 Habilitar a navegação privada

Habilitar a navegação privada previne o rastreamento do histórico de páginas web visitadas, pesquisas realizadas, e algumas informações utilizadas pelo preenchimento automático de formulários.

Habilitá-la pode proteger determinadas informações privadas contra uso indevido e impedir alguns sites de rastrear atividades do usuário através navegador Safari.

1. Executar o Safari
2. Pressionar o botão de abas do Safari. No iPhone ele encontra-se no canto inferior direito do Safari. No iPad ele encontra-se no canto superior direito.
3. Pressionar Privado

8.9 Impedir o rastreamento durante a navegação

Essa configuração instrui o navegador Safari a comunicar, para os sites aos quais ele se conecta, que não quer ser rastreado.

Tecnicamente, quando este recurso encontra-se habilitado, o navegador Safari é instruído a enviar um cabeçalho opcional em requisições HTTP realizadas a partir do navegador. Tal cabeçalho indica uma preferência de não ser rastreado por sites web; porém, ele possui natureza voluntária, ou seja, não há método ou técnica disponível para garantir que os sites web atuem em conformidade. Assim,

mesmo que este recurso encontre-se configurado não existem garantias de que sites honrarão tal preferência pela privacidade.

No entanto, um grande número de sites web são sim, aderentes a esta configuração. Por isso certamente há benefícios em habilitar tal recurso.

1. Pressionar Ajustes
2. Pressionar Safari
3. Na seção PRIVACIDADE E SEGURANÇA, ativar o recurso Não Rastrear, deslizando o controle para a direita

Capítulo 9

Referências

Neste capítulo, encontram-se listados alguns sites e livros que foram utilizados como fontes de informação para o desenvolvimento deste guia.

Cabe aqui uma ressalva sobre os endereços da internet. Mesmo tomando o máximo cuidado ao inseri-los neste capítulo, é natural que, com o tempo, eles sejam desativados ou mudem de endereço. Ou seja, alguns dos endereços utilizados correm o risco de se tornarem inválidos, ou "quebrados". Para os leitores, sugere-se pesquisar no Google pelos endereços atuais, caso algum link abaixo esteja quebrado.

9.1 Google Android 6.0 (Marshmallow)

A maioria das recomendações descritas aqui foi baseada no livro digital Android 6 User Guide. Este livro encontra-se disponível gratuitamente na Play Store, no seguinte endereço:

https://play.google.com/store/books/

Parte da recomendação sobre encriptação dos dispositivos Android teve como base um artigo do site Ars Technica, que pode ser visualizado no seguinte endereço:

http://arstechnica.com/gadgets/2016/03/why-are-so-few-android-phones-encrypted-and-should-you-encrypt-yours/

Ainda obre a encriptação, caso o leitor necessite de mais informações sobre a relevância (ou não) de se proteger as informações armazenadas no dispositivo, ele pode acessar a seguinte página:

http://security.stackexchange.com/questions/10529/are -there-actually-any-advantages-to-android-full-disk-encryption

Mais informações a respeito da importância de se configurar senhas de bloqueio em dispositivos podem ser acessadas no seguinte endereço:

https://www.teamsid.com/the-importance-of-having-a-secure-password-infographic/

9.2 Apple iOS 10

A maioria das recomendações descritas aqui foram baseadas no site de suporte da Apple, que encontra-se disponível no seguinte endereço:

http://support.apple.com/

O recurso Find my iPhone pode ser acessado no seguinte endereço:

http://www.apple.com/icloud/find-my-iphone.html

Com relação à eliminação de todas as informações armazenadas no dispositivo iOS, uma boa fonte de consulta é o livro iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Mais detalhes sobre este livro podem ser encontrados no seguinte endereço:

http://textbooks.elsevier.com/web/product_details.aspx?isbn=9781597496599

Com relação ao recurso para impedir o rastreamento durante a navegação, mais detalhes sobre a iniciativa *Do Not Track* podem ser encontrados nos seguintes sites:

- Do Not Track - Universal Web Tracking Opt Out (http://donottrack.us/)
- W3C Tracking Protection Working Group (http://www.w3.org/2011/tracking-protection/)
- Do Not Track — Electronic Frontier Foundation (https://www.eff.org/issues/do-not-track)