PROTEGENDO SEU TELEFONE CELULAR

VERSÃO 0.3, 2022-11

C. A. Heckler

RESUMO

O roubo de celulares é um crime frequente, e recentemente tem sido comum o roubo de aparelhos desbloqueados, com invasão de contas (inclusive bancárias) acontecendo poucos minutos após a subtração do aparelho. Esse guia reúne algumas práticas de segurança para minimizar a chance de danos ou prejuízo nesse tipo de crime. Algumas das instruções fornecidas são voltadas para o sistema iOS da linha iPhone, mas funcionalidades equivalentes existem em dispositivos Android.

VERSÃO MAIS ATUALIZADA

A última versão desse documento pode ser baixada sempre nesse link:

https://github.com/heckler/seguranca/raw/main/protegendo-celular.pdf

ÍNDICE

Introdução 2
Configurando uma senha no SIMCARD 3
Desabilitando a Pré-visualização de notificações 4
Restringindo o Acesso a Apps Sensíveis 5
Ativando a Confirmação em Duas Etapas no WhatsApp 6
Histórico de Revisões 7

INTRODUÇÃO

Esse documento é um pequeno guia com boas práticas de segurança para proteger o seu telefone celular e, principalmente, os seus dados e suas contas contra vários possíveis ataques, como ter o aparelho roubado, ou senhas vazadas em um site na internet

Nem todas as dicas oferecidas aqui se aplicam a todo mundo. Por exemplo, dicas para dificultar o uso da sua linha telefônica ou dificultar a clonagem do WhatsApp provavelmente são de interesse de todos. Já um incremento da segurança do seu perfil do Facebook ou Instagram pode não ser necessário se você raramente usa esses serviços, ou ser extremamente importante caso você tenha um pequeno negócio que use um desses serviços para divulgação e contato com clientes.

Sempre que possível junto a cada uma das sugestões oferecidas há uma explicação do risco que essa sugestão tenta minimizar, o que deve facilitar a decisão sobre adotar ou não uma determinada prática.

Finalmente, esse guia é um trabalho em andamento e novas versões são publicadas com alguma frequência. Consulte o link na primeira página para baixar a versão mais recente; a lista de alterações encontra-se na última página.

CONFIGURANDO UMA SENHA NO SIMCARD

RISCOS DE UM SIMCARD SEM SENHA

O cartão SIM (ou SIMCARD - Subscriber Identity Module) é o "chip" que contém as informações da linha telefônica. Se ele for removido do seu aparelho e instalado em outro, o criminoso tem acesso imediato à sua linha telefônica e mensagens SMS, podendo com isso (por exemplo) ativar o *WhatsApp* em outro aparelho, ou resetar senhas de contas como email, iCloud e até mesmo *home banking*.

É possível proteger a linha e o cartão SIM ativando uma senha de segurança que será solicitada toda vez que o seu telefone for ligado/re-iniciado, ou caso o cartão seja removido e inserido em outro celular.

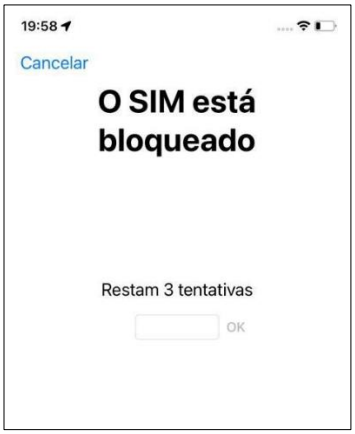
Os cartões SIM vêm da operadora com uma senha padrão (ver abaixo), e é importante trocar essa senha por uma outra, que seja única e secreta – a senha padrão da operadora é de conhecimento público.

COMO ATIVAR A SENHA DO SIMCARD NO IPHONE

Para ativar a senha, siga os seguintes passos:

- Entre em: Ajustes > Celular > PIN do SIM
- Toque no botão para ativar a opção "PIN do SIM"
- Ao ser solicitado, entre o PIN configurado no SIMCARD
    - Caso você nunca tenha configurado um PIN, use o PIN padrão da sua operadora:
        - Vivo: **8486**
        - TIM: **1010**
        - Claro: **3636**
- Se você nunca trocou o PIN do seu SIMCARD, o PIN padrão da operadora (acima) não é seguro, porque os criminosos conhecem essas senhas; siga o próximo passo para trocar
- Clique em "Alterar PIN"
    - Entre o PIN atual (o PIN padrão da operadora, acima)
    - Escolha um novo PIN e digite ele
    - Digite novamente o novo PIN para confirmar
- Pronto, seu cartão SIM está protegido com uma senha que só você conhece
- **Anote essa senha em um local seguro** em casa, pois caso seja perdida pode ser necessário solicitar um novo cartão para a sua operadora de telefonia.

TESTANDO A SENHA DO SIMCARD



Uma maneira simples de testar a nova senha é desligar e ligar novamente o celular. Ao ligar o cartão inicia bloqueado e é necessário informar a senha para desbloquear e passar a usar as funções de telefone celular.

A outra forma de testar é remover o SIMCARD do iPhone e inserir em outro aparelho. Da mesma forma, vai ser necessário informar a senha antes de poder usar a linha no aparelho.

Importante: se você digitar o PIN errado 3 vezes o cartão será bloqueado. Para desbloquear é preciso usar o código PUK (Personal Unlock Code), um código secreto de 8 dígitos (normalmente) que vêm junto com o SIMCARD quando a linha é adquirida. Se você não possui o PUK e bloqueou seu SIMCARD, entre em contato com a operadora de telefonia.

DESABILITANDO A PRÉ-VISUALIZAÇÃO DE NOTIFICAÇÕES

RISCOS DA VISUALIZAÇÃO DE MENSAGENS

Se o celular é roubado, mesmo sem desbloqueá-lo, alguém pode tentar resetar a senha do seu e-mail (ou home banking!) usando uma confirmação por SMS recebida no celular. Se o conteúdo das notificações é visualizado mesmo com o celular desbloqueado, o atacante consegue acesso ao código solicitado. Para evitar isso, o conteúdo das notificações deve ser exibido apenas com o celular desbloqueado. Com celulares que suportam FaceID, basta olhar para a tela para desbloquear, então esse ajuste não causa grande desconforto. Com TouchID, é necessário tocar o dedo no leitor biométrico para visualizar o conteúdo das notificações.

DESABILITANDO A PRÉ-VISUALIZAÇÃO DE NOTIFICAÇÕES

Para desabilitar a pré-visualização de notificações com o celular bloqueado, siga os seguintes passos:

- Acesse Ajustes > Notificações > Pré-visualizações.
- Mude para a configuração Quando Desbloqueado.

Como pode ser visto abaixo, se o celular estiver bloqueado (cadeado fechado), o conteúdo da mensagem não é exibido; mas basta olhar para o celular para desbloqueá-lo (usando FaceID) que o conteúdo completo da notificação é mostrado.

Celular bloqueado

Celular desbloqueado

RESTRINGINDO O ACESSO A APPS SENSÍVEIS

RISCO ENVOLVIDO

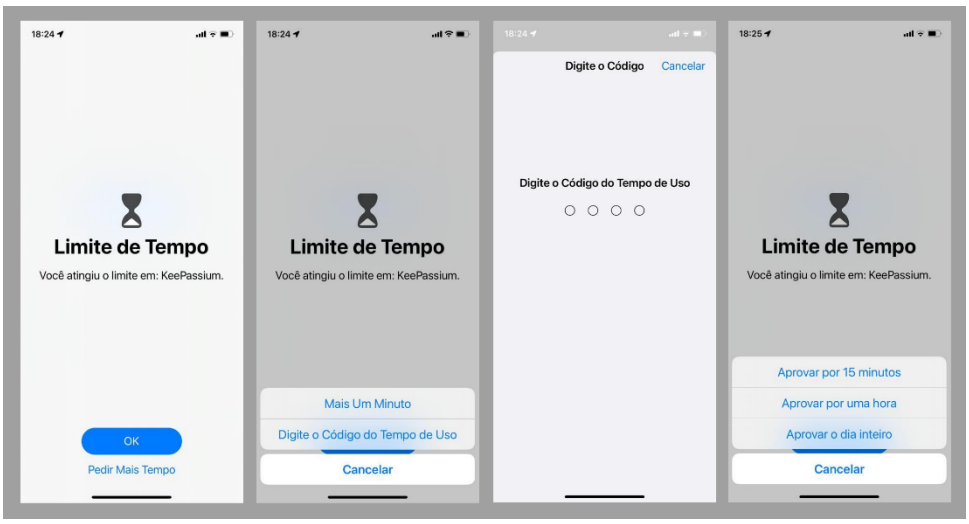
Existem apps como home banking, app de corretora ou outros que são considerados sensíveis por envolver transações monetárias. Esses apps você não acessa com muita frequência, e merecem uma camada adicional de proteção. Se um ladrão lhe roubar o celular desbloqueado, ele vai continuar mexendo na tela constantemente para evitar o bloqueio automático, e o próximo passo vai ser tentar iniciar um reset de senha no seu app do banco. Para evitar isso é recomendável uma camada extra de segurança para acessar certos aplicativos.

PROTEGENDO O ACESSO AOS APPS MAIS SENSÍVEIS

A Apple não oferece um mecanismo de proteção para o acesso a aplicativos individuais, mas é possível usar as restrições de Tempo de Uso para esse fim. Para isso, siga os seguintes passos:

- O primeiro passo consiste em ativar a funcionalidade:
  - Acesse Ajustes > Tempo de Uso.
  - Toque em Ativar Tempo de Uso.
  - Role para baixo e toque em Continuar.
  - Selecione a opção Este iPhone é Meu.
- Feito isso, defina um código para o ajustes
  - Acesse Ajustes > Tempo de Uso novamente
  - Toquem em Usar Código do Tempo de Uso.
  - Informe e confirme o código.
  - **Importante**: use um código diferente do código de desbloqueio do celular.
- Defina um limite para os aplicativos sensíveis
  - Acesse Ajustes > Tempo de Uso.
  - Toque em Limites de Apps.
  - Toque em Adicionar Limite.
  - Escolha e selecione todos os apps sensíveis usando as listas mostradas na tela.
  - Depois de selecionar os apps, toque em Seguinte.
  - Defina o tempo: como não é possível definir um limite de zero minutos, escolha a menor opção: 1 min.
  - Selecione a opção Bloqueio ao Fim do Limite.
  - Toque em Adicionar para criar o limite.

Com essa opção ativa, quando um dos aplicativos na lista esgotar o seu limite diário (1min), você vai ter a opção de continuar usando por mais um minuto, ou então entrar o código configurado acima (que deve ser diferente do código de bloqueio do celular). Se você informar o código correto, pode "desbloquear" o app por 15min, 1h ou o dia inteiro. Normalmente 15min ou 1h é o bastante para usar o app e não correr riscos.



ATIVANDO A CONFIRMAÇÃO EM DUAS ETAPAS NO WHATSAPP

RISCOS DE NÃO TER CONFIRMAÇÃO EM DUAS ETAPAS ATIVA

A "clonagem de WhatsApp" ocorre quando alguém ativa a sua conta de WhatsApp em outro aparelho, sem a sua autorização, normalmente para tentar obter dinheiro dos seus contatos. Já foi um crime mais comum, mas ainda acontece com alguma frequência. Isso é possível porque por padrão o WhatsApp não possui uma senha de ativação, dependendo apenas de uma mensagem SMS – que pode ser interceptada por clonagem de cartão SIM, com auxílio de funcionários das operadoras, ou outros métodos. A forma de se evitar esse risco é ativando a chamada "Confirmação em duas Etapas" do WhatsApp, usando uma senha de ativação – nesse caso o código enviado por SMS é a "primeira etapa", e a senha é a "segunda etapa".

COMO ATIVAR A CONFIRMAÇÃO EM DUAS ETAPAS

Para configurar a senha de ativação no WhatsApp basta fazer o seguinte

- No aplicativo do WhatsApp, clicar na aba Configurações entre as opções na base da tela
- Clicar em Conta > Confirmação em duas etapas
- Clicar em Ativar
- Escolha uma senha de ativação que somente você conheça
- Use preferencialmente uma senha diferente daquela que você usa para desbloquear o celular
- Memorize a senha: ela vai ser solicitada de tempos em tempos pelo aplicativo
- Anote essa senha em um local seguro: um aplicativo de senhas ou um cofre ou pasta em casa
- Após digitada e repetida a nova senha vai ser solicitado um endereço de e-mail
    - Adicionar um e-mail de recuperação é uma boa opção para o caso de você esquecer a senha.
    - MAS, se esse e-mail estiver configurado para ser lido no celular, a segurança do WhatsApp acaba sendo a mesma do celular, então é interessante usar um endereço de e-mail que você não tenha configurado no celular.
    - Pode-se também pular essa etapa e não informar um e-mail; nesse caso é fundamental salvar com cuidado a senha.

COMO PROCEDER SE A SENHA DE ATIVAÇÃO FOR PERDIDA OU ESQUECIDA

Caso você ative a Confirmação em Duas Etapas e esqueça a senha de ativação – ou sofra um acidente e esteja impossibilitado de compartilhar a senha, é possível remover ou redefinir o PIN, mesmo sem ter acesso ao e-mail que foi configurado (ou caso nenhum e-mail tenha sido configurado). Porém, para isso é necessário esperar **7 dias**; isso serve para impedir que alguém tenha acesso à sua conta em caso de roubo do celular – em tese dentro de 7 dias você mesmo já configurou a conta num novo aparelho.

Para iniciar a recuperação, quando for solicitado o PIN, clique em Esqueceu o PIN? ao ser solicitado. Caso tenha sido configurado um e-mail será enviada uma mensagem para resetar o PIN; caso não haja e-mail configurado (ou não tenha mais acesso ao e-mail) será necessário esperar 7 dias para completar o processo.

HISTÓRICO DE REVISÕES

Data	Versão	Alterações
2022-09-26	0.1	Primeira versão do documento: PIN no SIMCARD
2022-10-12	0.2	Autenticação de duas etapas no WhatsApp
2022-11-02	0.3	Tempo de uso e pré-visualização de notificações