CHECKLIST DE SEGURANÇA DIGITAL

*****

UM CHECKLIST COMPLETO DE COMO PROTEGER SUAS CONTAS E EVITAR SER HACKEADO.

SIGA: @TIAGOTESSMANN

01 COLOQUE SENHA NO SEU CHIP

*****

Coloque senha no SIM chip. Em um caso de roubo de celular onde o ladrão poderia colocar seu chip em outro celular para hackear suas contas, ele não conseguirá usar o chip sem saber o PIN que você criou. O PIN é uma senha com alguns números que você irá criar.

Na internet você encontra vários tutorias de como fazer isso diretamente pelas configurações do seu celular, caso não consiga, entre em contato com sua operadora para descobrir como fazer isso. Compre um novo CHIP case seja necessário, sua segurança vale mais que R$ 25,00.

02

TODAS AS OPERADORAS SÃO VULNERÁVEIS, MAS A CLARO É A PIOR.

*****

Em 90% das mensagens que recebi de pessoas que foram hackeadas, a Claro era a operadora. Então recomendo trocar de operadora ou ficar ainda mais atento ao checklist de segurança.

A minha operadora é VIVO, porém a CLARO fez a portabilidade e quando isso acontece, a VIVO não tem controle.

FUJA DA CLARO.

03

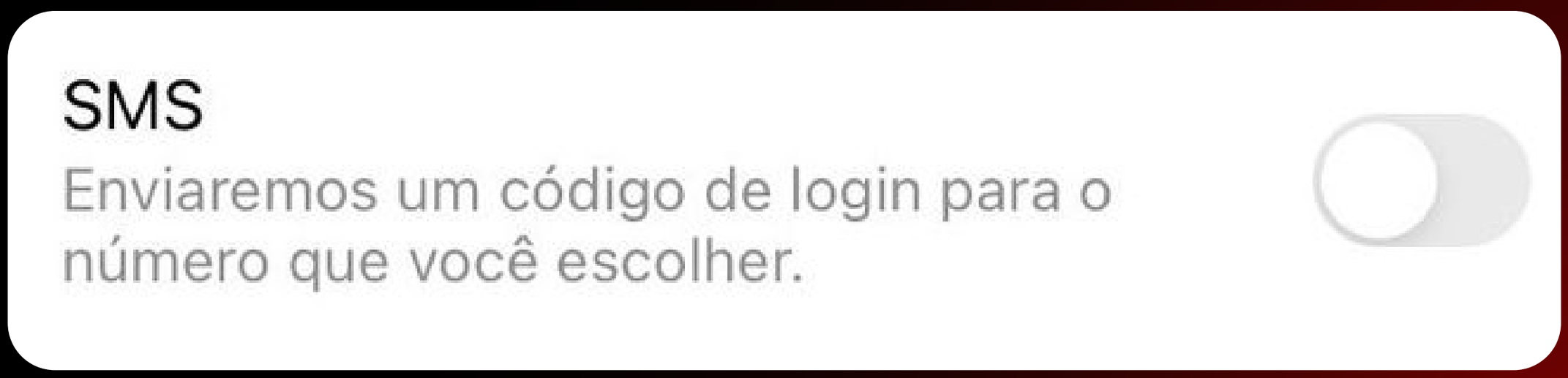
*****

REMOVA A AUTENTICAÇÃO DE 2 FATORES POR SMS DE TODOS SEUS APLICATIVOS E CONTAS DE E-MAIL.

É justamente por esse caminho que a maioria dos casos de hacking acontecem, por recuperação de senha por SMS.

Caso queira ter autenticação por SMS, considere colocar sua conta em PJ, é menos vulnerável que em PF.

Eu particularmente não confio na segurança das operadoras do Brasil, por isso que essa será minha última opção.



04 DESATIVE AS NOTIFICAÇÕES DE CELULAR COM A TELA BLOQUEADA

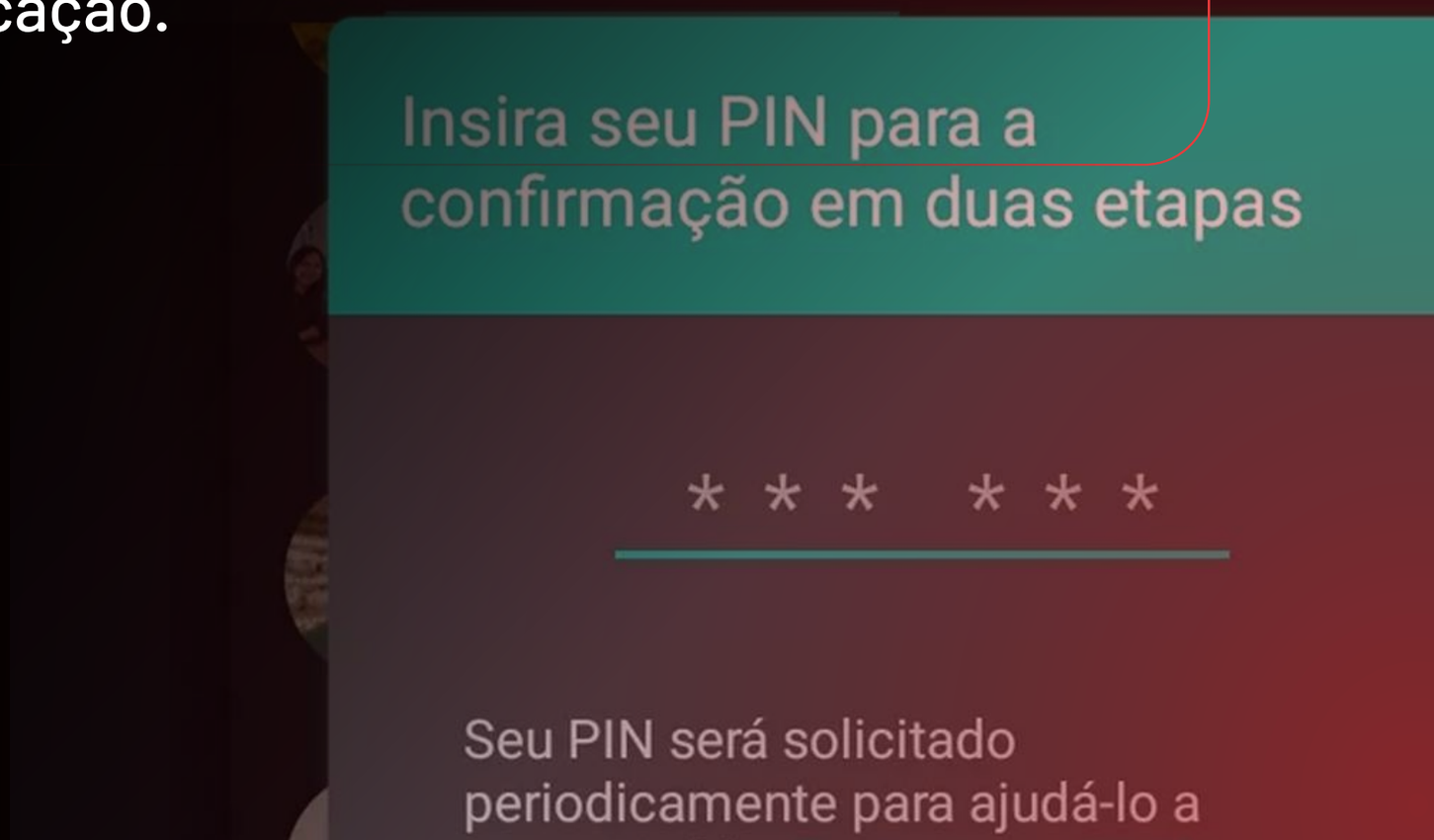
*****

Algumas notificações de mensagens mostram códigos de acesso, mesmo com a tela bloqueada.

05 HABILITE O PIN NO WHATSAPP E EM OUTROS APLICATIVOS

*****

Habilite o PIN em todos aplicativos que você puder, como WhatsApp, aplicativos de bancos e até mesmo o aplicativo de dupla autenticação.



06 USE UM GERENCIADOR DE SENHAS COMO O 1PASSWORD (É PAGO)

*****

Cada aplicativo seu precisa ter uma senha forte, mas é impossível gravar todas as senhas. Por isso é recomendado ter um gerenciador de senhas para criar senhas fortes, preenchê-las automaticamente e não correr o risco de esquecer alguma senha.

No gerenciador de senhas você tem uma senha mestre que dará acesso a todas as outras.

Há vários gerenciadores de senhas, o que eu uso é o **1Password** pela grande parceria e facilidade no uso nos dispositivos Apple.

Não use a mesma senha em diferentes serviços.

07 TENHA AUTENTICAÇÃO DE 2 FATORES POR APLICATIVO EM TODAS SUAS CONTAS

*****

Mas tome cuidado. A maioria dos aplicativos de dupla autenticação são vinculados ao seu telefone, então se você resetar o celular, perder ou ser roubado, você pode acabar não conseguindo mais acessar suas contas. Então escolha aplicativos que possuem alguma forma de backup ou funcionem através de senha mestre.

Uma boa opção é o **Authy (by twilio)**, que pode ser usado em múltiplos dispositivos ao mesmo tempo e seu vínculo é ao número de telefone e não ao dispositivo. Assim, caso você troque de celular ou perca, você conseguirá recuperar os códigos via número de telefone, mas só conseguirá acessar os códigos com sua senha mestre.

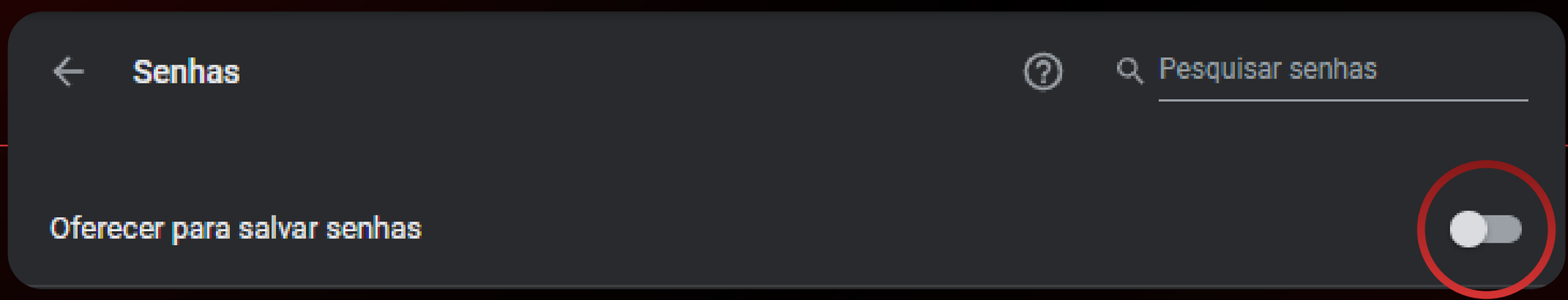
Um outra opção é o **Microsoft Authenticator** (esse é o que eu uso), pois você pode fazer o backup na nuvem.

Google Authenticator não é recomendado, pois se perder o celular fica difícil de recuperar.

08 NÃO SALVE NENHUMA SENHA FORA DO SEU GERENCIADOR DE SENHAS

*****

Não salve suas senhas no Chrome, Safari ou iCloud. Use aplicativos como o 1Password ou LastPass para salvar e gerenciar suas senhas.



09 EVITE COMPARTILHAR SENHAS PELO WHATSAPP, TELEGRAM, ETC

*****

A maneira mais segura de compartilhar senhas é através do seu gerenciador de senha. Lá você pode clicar em compartilhar e dar o link pra pessoa acessar a sua rede social, por exemplo, apenas clicando neste link. O interessante disso é que você pode limitar os acesso ou tempo de acesso através desse link.

10 ALTERE O NOME DOS SEUS CONTATOS

*****

Não facilite para os bandidos. Não use nomes como pai, mãe, irmão, esposa, amor, etc.

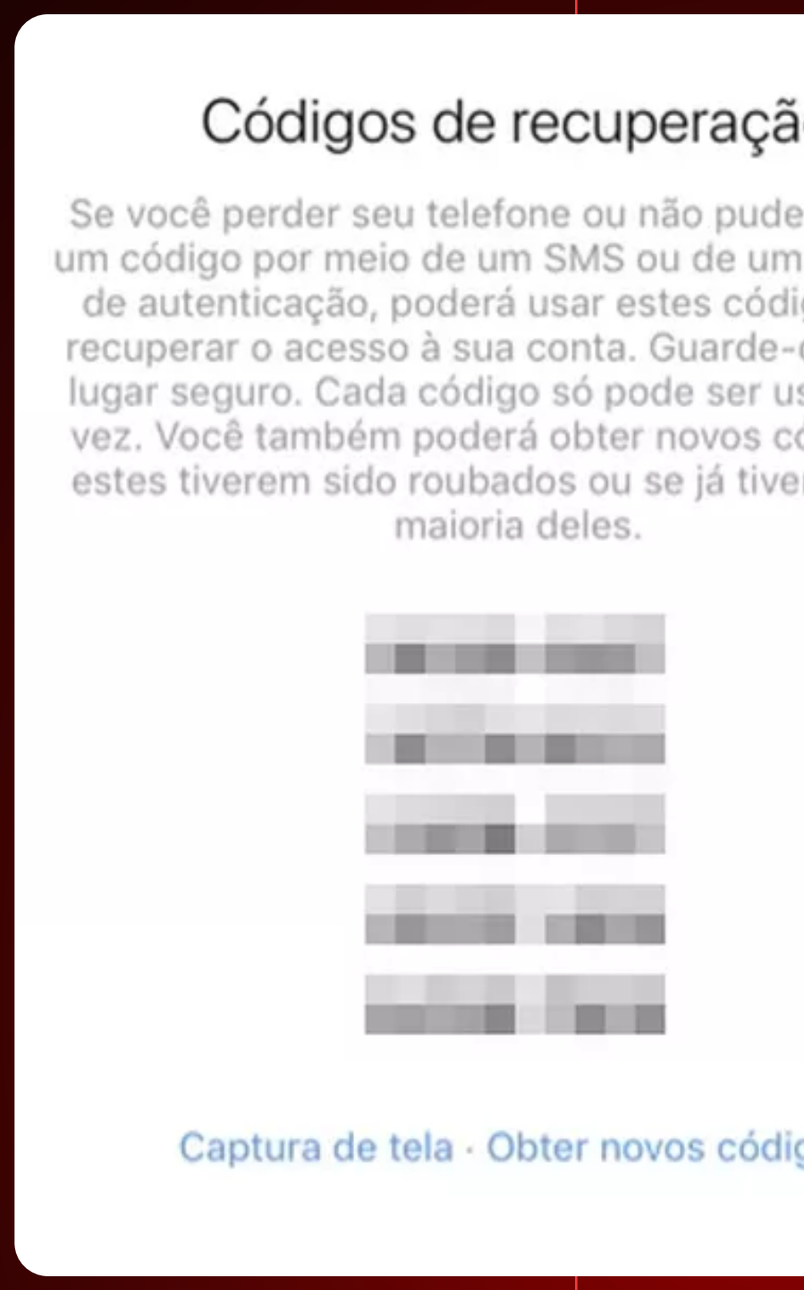
11 IMPRIMA 2 CÓPIAS DAS SENHAS BACKUP

*****

Contas importantes como Google, Microsoft, Facebook, Instagram tem senhas de backup ou código mestre para recuperação de contas.

Vá em “segurança” e imprima os “códigos backup”. Guarde um na sua casa em um lugar seguro e o outro dê pra alguém de confiança em uma pasta.

Caso roubem seu celular, computador, invada sua casa, mesmo assim há como recuperar suas contas.



12

*****

IMPRIMA O KIT EMERGÊNCIA DO SEU GERENCIADOR DE SENHAS

Você não pode perder de jeito nenhum o gerenciador de senhas, lá é onde está praticamente a sua vida.

Por isso os gerenciadores criaram o Kit emergência, que é um documento com suas senhas e chave mestre para recuperação de conta caso acessem ou você esqueça a senha mestre.

13 INSIRA E-MAIL DE RECUPERAÇÃO DE ALGUÉM DE CONFIANÇA E QUE PROTEGE MUITO A CONTA

*****

Contas importantes como Google, Microsoft, Facebook, Instagram tem a opção de inserir um e-mail de recuperação caso alguém invada a conta. Coloque alguém de confiança para recuperar.

Meu Instagram foi recuperado graças a isso.

14 DESCUBRA O QUÃO FORTE SUAS SENHAS SÃO

*****

Os gerenciadores de senhas já dizem o quão forte é sua senha, caso não tenha, use esse site: **https://www.security.org/how-secure-is-my-password/**

15 CUIDADO COM PHISHING

*****

“Se você seguir as dicas neste documento, estará praticamente imune ao phishing porque com a verificação de duas etapas é muito difícil alguém acessar a sua conta.

Porém, fica a dica: suspeite de e-mails estranhos que pedem informações pessoais. Confira sempre de quem veio o e-mail (prestando atenção no domínio do endereço) e o conteúdo.”

Além disso, sempre verifique os Links (URL) dos sites que você acessa. Alguns sites de phising clonam o visual de outros sites como redes sociais e sites bancários de forma identica, fazendo com que pareça que você está acessando o site oficial, por isso, sempre verifique a URL do site.

Fonte: Tecnoblog

16

CHEQUE A ATIVIDADE DA SUA CONTA DE TEMPOS E TEMPOS

*****

Google:

https://myaccount.google.com/security?utm_source=my-activity&utm_medium=home&utm_campaign&pli=1#activity

Facebook:

https://www.facebook.com/settings?tab=security&section=sessions&view

17

MUDE SUAS SENHAS REGULARMENTE

*****

Algumas contas dizem qual foi a última vez que você alterou a senha. O ideal é alterar de vez em quando.

18 EVITE REDES WI-FI PÚBLICAS

*****

“Redes Wi-Fi estão por todos os lados: restaurantes, shoppings, ônibus rodoviários, hospitais, lojas e por aí vai. Mas, quanto menos você usar essas redes, melhor. Isso porque é perfeitamente possível rastrear ou coletar dados de navegação por meio delas.

Além disso, algumas redes Wi-Fi públicas exigem cadastro ou check-in no Facebook. Os dados provenientes dessas ações podem ser usados para fins obscuros.

Por isso, sempre que possível, dê preferência a um plano de dados 3G ou 4G para o seu celular.”

Fonte: Infowester

VPN pode ser uma solução, eu não utilizo, mas mantém seu IP anônimo na internet.

19

*****

SENHA ADICIONAL A SENHA PADRÃO QUE NÃO ESTÁ EM NENHUM LUGAR

O que acontece se alguém acesse meu gerenciador de senhas? Já era! Terá acesso a todas as suas contas. É claro que não terá seu celular para autenticação de 2 fatores, isso já dificulta muito a ação do hacker. Porém tem muitas contas que não tem autenticação e é complicado saber que alguém pode acessá-las.

Como resolver isso e deixar suas contas realmente protegidas, mesmo que alguém descubra sua senha mestre?

Através da senha adicional, vou explicar:

Imagine que você criou senha para 3 serviços diferentes:
1. Google: Moam&ˆ9aofmma**@150115**
2. Facebook: 420dkamAD!**@150115**
3. Instagram: dvmpap( )dkaam4**@150115**

No final de cada senha, adicione uma senha padrão sua, que não está escrita em nenhum lugar, só você sabe. (Imprima essa senha em um documento, é claro)

Então no gerenciador a senha será: **“Moam&ˆ9aofmma”** e aí você completa com sua senha padrão secreta:
“Moam&ˆ9aofmma**@150115**”

Mesmo que acessem seu gerenciador, será impossível acessar qualquer conta sua.

20

*****

HAJA RÁPIDO, VELOCIDADE É IMPORTANTE PARA RECUPERAR SUAS CONTAS.

O que me ajudou a recuperar minhas contas foi que eu parei tudo o que estava fazendo na hora e fui atrás para resolver isso.

Felizmente eu tenho um time que me ajudou neste processo, sozinho talvez eu não teria conseguido. Por isso é importante que você faça todos os passos acima.

Imagine se você está viajando, em um lançamento ou em uma festa importante, sim, isso pode destruir seu dia, então faça isso agora e evite que o pior aconteça.

COMPARTILHE ESSE DOCUMENTO COM O MAIOR NÚMERO DE PESSOAS POSSÍVEL.

*****

E NÃO ESQUEÇA DE SEGUIR:
@TIAGOTESSMANN NO INSTAGRAM