DICAS DE PRIVACIDADE E COMPORTAMENTO EM REDES SOCIAIS PARA JORNALISTA

...

FÁBIO GUSMÃO
EDITOR O GLOBO/EXTRA
2018

Android é foco dos ataques a dispositivos móveis no Brasil

O **Brasil aparece em 5º lugar em malware para plataforma móvel**, atrás de Japão e Estados Unidos, com cerca de 10% de tentativas de infecções a dispositivos móveis em relação ao total de ameaças detectadas.

O **Android** é o mais utilizado no Brasil e o mais vulnerável, com **99,9% das tentativas de ataque**. Do total de malwares em dispositivos móveis detectados na América Latina e no Caribe no primeiro trimestre de 2017, 28% deles eram malwares para dispositivos Android.

Malware é qualquer tipo de programa de computador, celular, entre outros, que seja capaz de se reproduzir, que se instale sozinho, roubando dados ou causando transtorno ao usuário da máquina.

PHISHING

O mais antigo tipo de golpe digital

É uma forma de cibercrime.
O nome phishing é um erro ortográfico consciente da palavra pesca e envolve roubar dados confidenciais do computador de uma pessoa e, subsequentemente, usar os dados para roubar a vítima.
O cibercriminoso cria uma réplica de uma instituição financeira ou site de comércio on-line, por exemplo. As vítimas são atraídas para o site e induzidas a divulgar seu login, senha, número de cartão de crédito em um formulário falso.
Depois o criminoso utiliza os dados para roubar o dinheiro.

Fonte: Kaspersky

PHISHING

O mais antigo tipo de golpe digital

Vítimas de golpe no Brasil: 48 milhões, quase 25% da população

30% dos internautas brasileiros sofreram ao menos uma tentativa de golpe em 2017

Em 2018, até agora, já está em 23%

Fonte: Kaspersky

PHISHING

O mais antigo tipo de golpe digital

Tipos de ataques phishing na América Latina (janeiro e agosto de 2018)

- Bancos: 69,28%
- Portais de internet globais: 12,75%
- Serviços web (e-mail, redes sociais): 10,95%
- E-commerce: 4,14%
- Outros: 2,88%

Fonte: Kaspersky

Mais de 90% dos ciberataques chegam por um e-mail de phishing.

Abrimos mensagens por curiosidade: 14%,

Por medo: 13%

Por urgência: 13%

PHISHING

O mais antigo tipo de golpe digital

- smishing (phishing por SMS)
- golpes de WhatsApp (cupons e sites falsos)
- redes sociais (posts promovidos, descontos)
- links maliciosos no Google AdWords (busca de palavra-chave)
- chamadas telefônicas convencionais (passando-se por empresas)
- domínios falsos (com códigos ASCII e caracteres unicode de outros idiomas)

Fonte: Kaspersky

Houve dois avanços do phishing:

Aumento do uso de certificado digital (SSL) que inclui HTTPS em sites maliciosos.

Domínios falsos que usam caracteres unicode com letras de alfabetos russos, tailandês e cirílico. Se parecem com as do latino.

-

FORMA DE DETECÇÃO E PROTEÇÃO

Consultar o Whois (Registro.br)

Saber quem é o dono do domínio

CATÁLOGO DE FRAUDES

Rede Nacional de Ensino e Pesquisa

Desde 2008, a RNP disponibiliza para consulta todas as fraudes identificadas pelo CAIS sobre os principais golpes que estão em circulação.

RNP
REDE NACIONAL DE ENSINO E PESQUISA

https://www.rnp.br/servicos/seguranca/catalogo-fraudes

ANTIVÍRUS PROTEGE MESMO?

Sim e não.

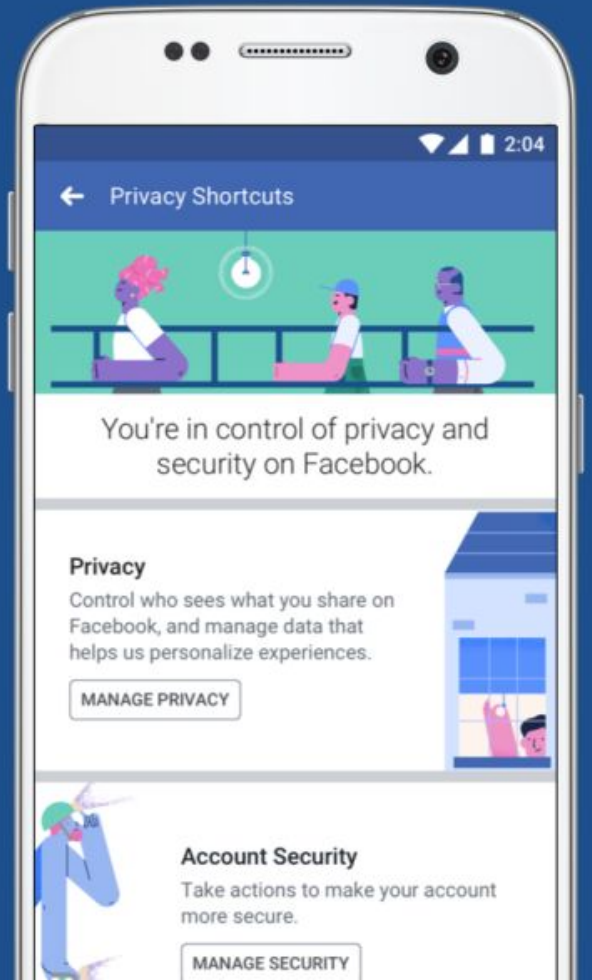
Antivírus mobile: alerta sobre URLs suspeitas cadastradas no seu banco de ameaças. O link é bloqueado automaticamente ao abrir no navegador.

Entretanto, quando você está dentro de um APP (WhatsApp, por exemplo) o vírus não está sob vigilância. As mensagens dentro do WhatsApp são criptografadas. Apenas quando um link dentro do APP é clicado o antivírus pode pegar.

Golpe novo, URLs novas. Isso pode dificultar a detecção pelo antivírus, que não tem o banco de dados atualizado.

Se o usuário continua tentando abrir o link (esse comportamento é comum) ou não mantiver o antivírus atualizado, não há o que fazer. O caminho fica livre para golpistas digitais.

facebook


2:04
Privacy Shortcuts
You're in control of privacy and security on Facebook.
Privacy
Control who sees what you share on Facebook, and manage data that helps us personalize experiences.
MANAGE PRIVACY
Account Security
Take actions to make your account more secure.
MANAGE SECURITY

Nome, endereço e data de nascimento: tudo isso junto facilita o trabalho de quem quer ter acesso a outros detalhes pessoais.

Com o seu nome, a sua casa e com a sua data de nascimento é possível ter acesso a outros dados pessoais.

Disponibilizar o número de celular na sua página do Facebook:

Apague quem realmente não é seu amigo real na sua rede. Você estará mais seguro com um círculo de amizades mais restrito, com mais controle. Um stalker, por exemplo, terá mais dificuldade de ver seus hábitos.

Fotografias dos seus filhos ou de outras crianças da sua família: seja cuidadoso, você não sabe quem terá acesso ao conteúdo. Assim como a localização da escola dos seus filhos ou de outras crianças da sua família.

Cuidado com os desabafos na rede. Sua TL nã deve virar um muro de lamentações, principalmente se elas são relacionadas ao seu trabalho, bem como de questões íntimas e familiares.

Evite colocar a localização das suas publicações É sempre um risco divulgar o lugar onde tirou as suas fotos, vídeos e publicações. Local onde mora, jamais!

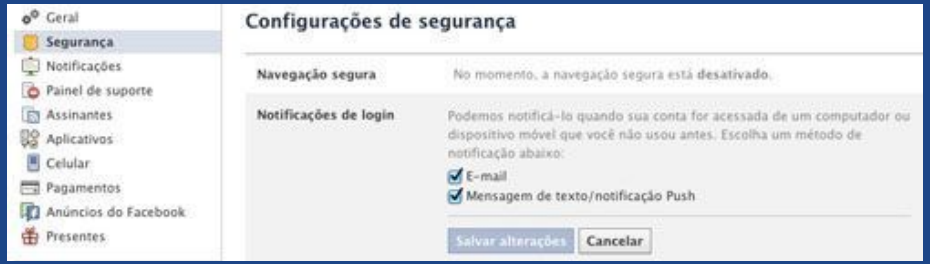
O dia e o destino das suas férias. Evite publicar.

Proteja a identidade ou os vínculos de relacionamento e familiares.

Como melhorar a segurança no Facebook

O protocolo HTTPS protege de roubo de senhas e de contas. Marque a navegação segura nas configurações de segurança. Nas configurações de conta.

Notificação por e-mail ou celular quando tentarem acessar sua conta. Em segurança, selecione as duas opções e salve. Você será avisado sobre a tentativa de invasão das duas formas.

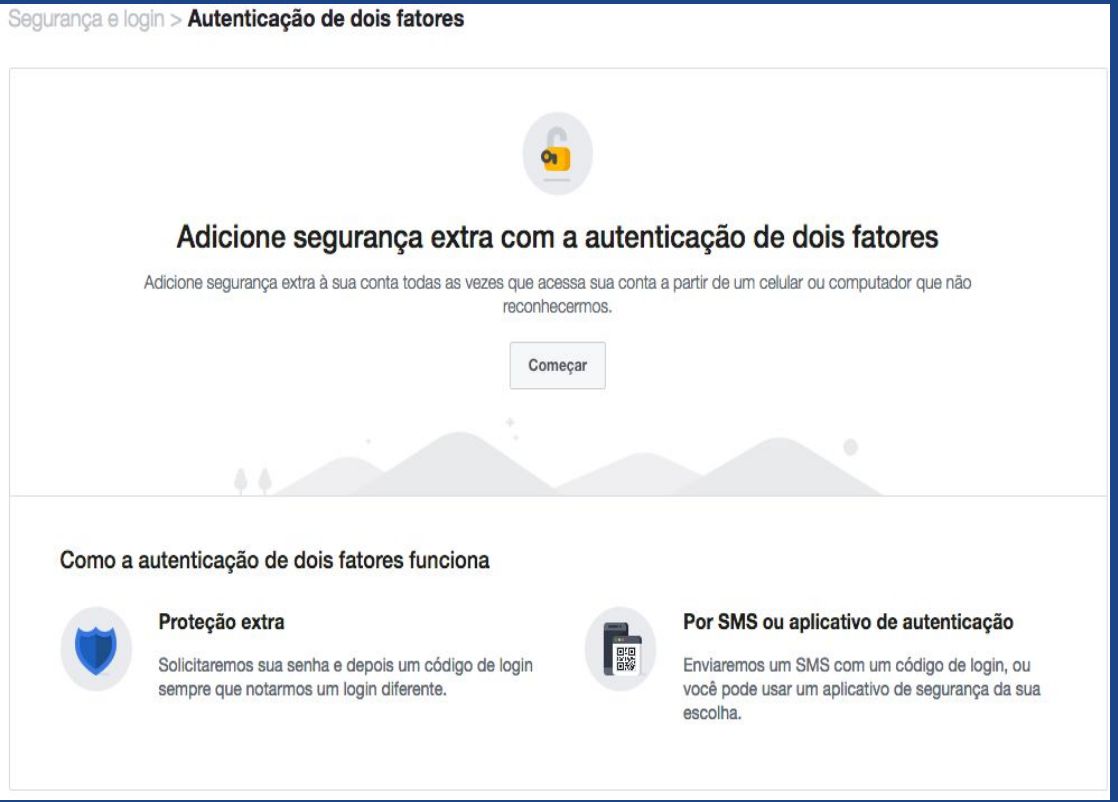


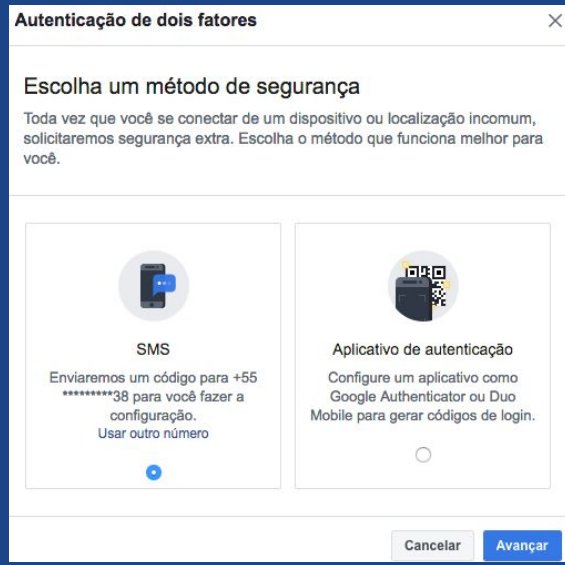
Registre seu número de telefone nas configurações. Você irá receber notificações no celular sempre que tentarem acessar sua conta por meio de outro dispositivo. Marque a opção "Aprovações de login", depois selecione a o item que pede um código de segurança sempre que um computador ou dispositivo desconhecido tentar acessar sua conta.

Como melhorar a segurança no Facebook

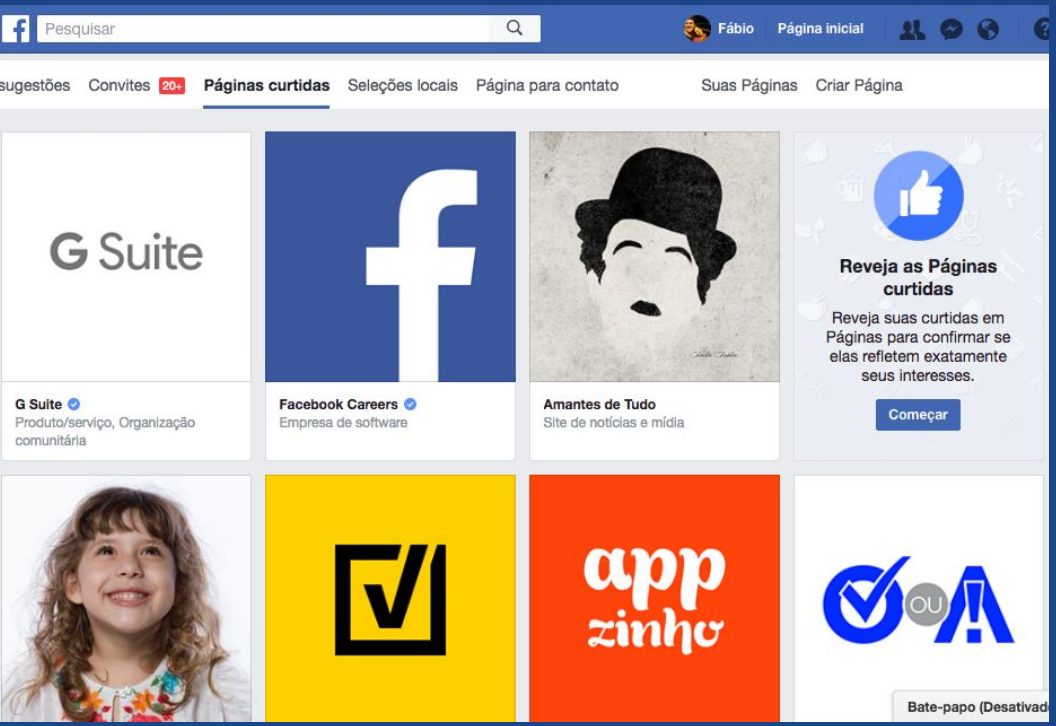
Cadastre os dispositivos que costuma usar: vá em "Dispositivos reconhecidos" e selecione. O FB enviará um SMS com código de segurança toda vez que você acessar de um navegador, dispositivo ou computador diferente.

Segurança no FB: autenticação de 2 fatores



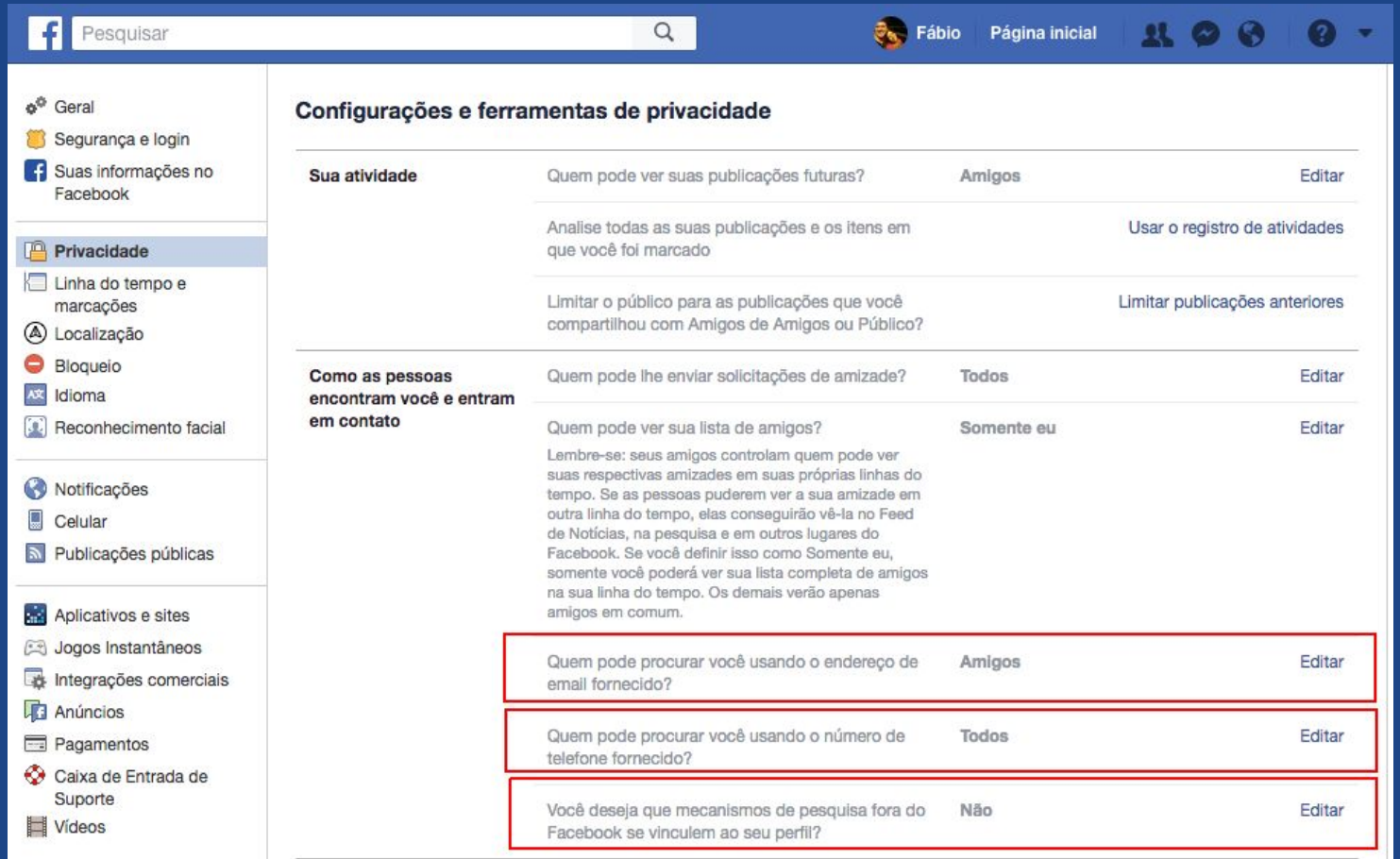


PÁGINAS CURTIDAS NO FB: COMO DESCURTIR



- Clique na opção **“Páginas”: FICA NO** no menu à esquerda do feed de notícias
- Clique em **“Páginas Curtidas”:** No topo da página.
- Vá em **“Reveja as Páginas curtidas”:** clique em **“Começar”**.
- Marque as páginas da sua lista que deseja descurtir. Clique em **“Avançar“**.
- Aparecerá a tela das páginas marcadas: clique em **“Salvar”.**

Dificultar ser descoberto no FB



Dificultar ser descoberto no FB

NL | FR | EN

stalkscan.com

All 'public' info Facebook doesn't let you see

Enter the link of the profile you want to check

https://facebook.com/yourprofile

Attention: this tool does **not** violate Facebook's privacy settings. 'Only me' stays 'only me'.
It only shows hidden content you have access to, on Facebook.

Tweet

Avalable options

- Everything
- Persons
- Gender
- Age
- Relationship status

Profile

- Pictures
- Videos

Tags

- Pictures
- Videos
- Posts

Comments

- Pictures
- Videos
- Posts

Liked

People

- Family
- Friends
- Friends of friends
- Co-workers
- Classmates
- Locals

Interests

- Pages
- Political parties

INTELTECHNIQUES
By Michael Bazzell

OSINT TRAINING
PRIVACY CONSULTING
DIGITAL SECURITY

OSINT LINKS
SEARCH
FACEBOOK
TWITTER
INSTAGRAM
NAME
USER NAME
EMAIL
TELEPHONE
DOMAIN
IP ADDRESS
YOUTUBE
REVERSE IMAGE
REVERSE VIDEO
DOCUMENTS
PASTEBINS
LINKEDIN
MAPPING
COMMUNITIES
SOCIAL

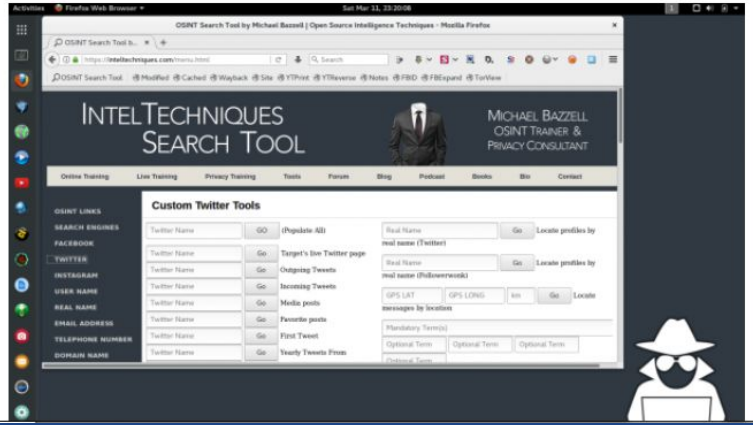
Online Internet Search Tool

Welcome to the new IntelTechniques Search Tool. Use the links to the left to access all of the custom search tools. The **OSINT LINKS** section contains hundreds of online search resources. Click any category to expand the selection. The **OSINT Linux build** can be found HERE.

Buscador: An OSINT Linux Virtual Machine

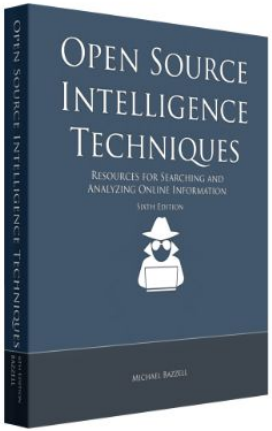
Buscador is an OSINT Linux Virtual Machine that is pre-configured for online investigations. It was developed by David Westcott and Michael Bazzell, and distributions are maintained on this page.

Download Buscador HERE



NEW OSINT GUIDE!

The Sixth Edition of the book on internet search techniques is now available. Click the book below for details.



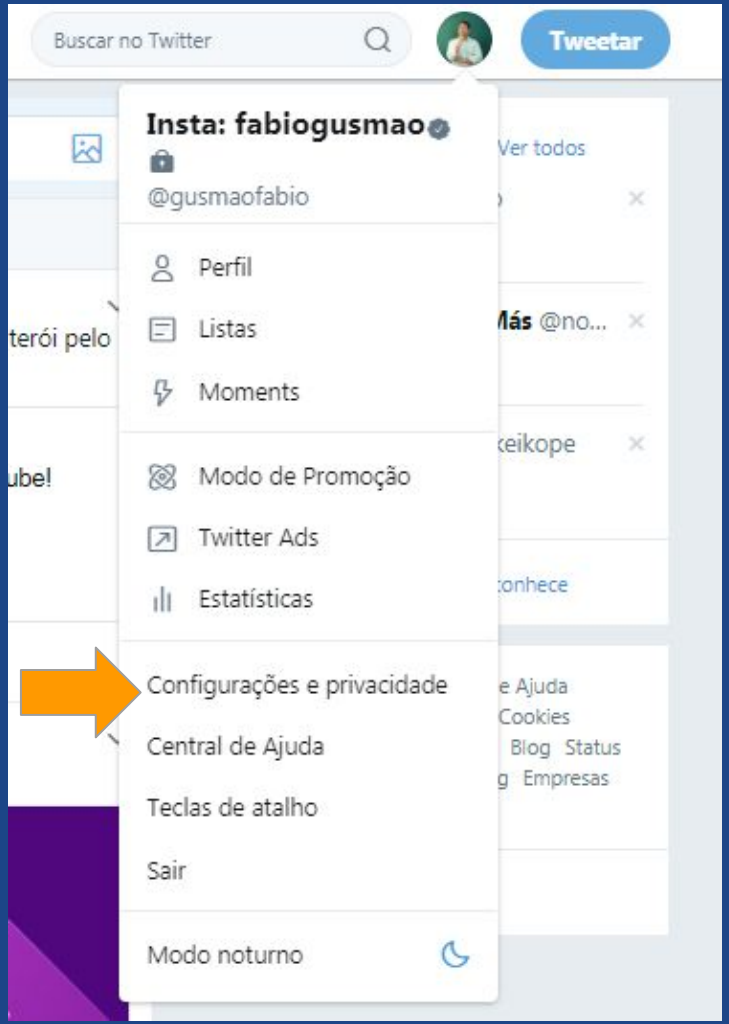
Free Newsletter

Enter your email address to subscribe to our free monthly newsletter:

Configurações de privacidade

E-mail e número de celular visíveis

Frequentemente, as melhores conexões no Twitter acontecem com as pessoas que você já conhece. Para ajudar você a estabelecer essas conexões, O Twitter usa o seu endereço de e-mail e número de celular para que outras pessoas possam descobrir sua conta. Você decide se outros usuários podem encontrá-lo no Twitter pelo seu número de celular ou endereço de e-mail. Basta ajustar suas configurações de visibilidade. Veja as instruções a seguir: Se você desativar as configurações que permitem que outras pessoas encontrem sua conta pelo seu endereço de e-mail ou número de celular, o Twitter também não usará sua lista de contatos (se você optou por carregá-la) para sugerir sua conta a outras pessoas.



Clique no botão Perfil e Configuração para poder acessar o botão Configurações conforme ilustra a imagem abaixo.

Clique em **Segurança e privacidade**.

Selecione o quer modificar.
Em segurança:
Verificar pedidos de seguidores.
Pode receber solicitações de verificação para o celular.
Pedir informações pessoais para redefinição de senha.

Em Privacidade:
Permitir ou não que marquem você em suas fotos, ou não.
Proteger seus Tweets para que somente os usuários que você permita os leiam.
Compartilhar a localização de onde você envia um Tweet.
Permitir que os outros lhe encontrem informando seu e-mail.
Personalizar seu Twitter conforme os sites que você visitou recentemente.
Receber anúncios personalizados baseados em informações compartilhadas por parceiros de publicidade do Twitter. (Considere que isto permite ao Twitter mostrar anúncios sobre temas que você tem mostrado interesse).
Receber mensagens diretas de qualquer pessoa, mesmo que ela não seja sua seguidora.


Instagram

fabiogusmao

563 publicações 2.252 seguidores seguindo 6.486

Fábio Gusmão
#Jornalista - Editor Digital. #Consultor em estratégia #digital. #Mediatraining.
t.co/qofI5pFa9g

Alterar senha

Aplicativos autorizados

Notificações

Privacidade e segurança

Sair

Cancelar

Busca

Email e SMS

Gerenciar contatos

Privacidade e segurança

Privacidade da conta

Conta privada

Quando sua conta é privada, somente as pessoas que você aprova podem ver suas fotos e vídeos no Instagram. Seus seguidores existentes não serão afetados.

Status da atividade

Mostrar status da atividade

Permita que as contas que você segue e todas as pessoas para quem envia mensagens possam ver quando você esteve online pela última vez nos aplicativos do Instagram. Quando essa opção estiver desativada, você não poderá ver o status de atividade de outras contas.

Compartilhamento de story

Permitir compartilhamento

Permita que as pessoas compartilhem seu story como mensagens

Comentários

Editar configurações de comentários

Fotos com você

Adicionar automaticamente

Adicionar manualmente

Editar configurações de comentários

Fotos com você

- (•) Adicionar automaticamente
- ( ) Adicionar manualmente

Escolha como deseja que as fotos com você sejam adicionadas ao seu perfil. Saiba mais sobre Fotos com você.

Dados da conta

Ver dados da conta

Autenticação de dois fatores

Desativar autenticação de dois fatores

Download de dados

Solicitar download

Ajuda com privacidade e segurança

Suporte

Autenticação de dois fatores

- [x] Exigir código de segurança

Com a ativação disso, enviaremos um código de segurança quando precisarmos de confirmação de que é você que está fazendo login.

Obter códigos de reserva

Os códigos de reserva são úteis caso você perca o acesso ao seu número de telefone e não consiga receber um código de segurança por SMS.

FICA O ALERTA: CELULAR

Grande quantidade de informações pessoais armazenadas: informações como conteúdo de mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, números de cartão de crédito e senhas costumam ficar armazenadas nos dispositivos móveis.

Maior possibilidade de perda e furto: em virtude do tamanho reduzido, do alto valor que podem possuir, pelo status que podem representar e por estarem em uso constante, os dispositivos móveis podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes.

Grande quantidade de aplicações desenvolvidas por terceiros: há uma infinidade de aplicações sendo desenvolvidas, para diferentes finalidades, por diversos autores e que podem facilmente ser obtidas e instaladas. Entre elas podem existir aplicações com erros de implementação, não confiáveis ou especificamente desenvolvidas para execução de atividades maliciosas.

Rapidez de substituição dos modelos: em virtude da grande quantidade de novos lançamentos, do desejo dos usuários de ter o modelo mais recente e de pacotes promocionais oferecidos pelas operadoras de telefonia, os dispositivos móveis costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados nele gravados.

Fonte: Cartilha de Segurança para Internet - CERT.br

FICA O ALERTA: CELULAR

- Instale um programa *antimalware* antes de baixar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;
- Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;
- Veja as notícias veiculadas no *site* do fabricante, principalmente as relacionadas à segurança;
- Cuidado ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e *plug-ins*. Procure usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação;
- Seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isto pode comprometer a sua privacidade.

Ao acessar redes:

- Cuidado ao usar redes Wi-Fi públicas;
- Mantenha o *bluetooth*, infravermelho e Wi-Fi desabilitados e as habilite quando for necessário;
- Configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").

Fonte: Cartilha de Segurança para Internet - CERT.br

55 21 - 9 8883-4638

fabiogusmao.com.br

Fábio Gusmão

Jornalista

fg@fabiogusmao.com

fabiogusmao33