Não é sorte,

é atitude!

Uma internet mais
segura em 5 dicas.

ATRIBUIÇÃO-SEMDERIVAÇÕES 4.0INTERNACIONAL (CC BY-ND 4.0)

VOCÊ TEM O DIREITO DE:

Compartilhar copiar e redistribuir o material em qualquer suporte ou formato.

DE ACORDO COM OS TERMOS SEGUINTES:

ATRIBUIÇÃO
Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de maneira alguma que sugira ao licenciante a apoiar você ou o seu uso.

SEM DERIVAÇÕES
Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

creativecommons.org/licenses/by-nd/4.0

globo | Toda atitude conta – Segurança da informação

Safernet

Que a Internet é um espaço
de oportunidades, diversão,
aprendizado, colaboração e tudo
mais, a gente já sabe, né?

Mas, por ser um ambiente tão vasto
e possibilitar o acesso de diversas
pessoas com diferentes objetivos,
precisamos estar atentos para nos
mantermos seguros e protegidos,
não é mesmo?

**E para ajudar você, sua família e
seus amigos a ficarem ligados e
se manterem seguros na Internet,
a Globo criou esse material com
5 dicas essenciais para que a sua
experiência nesse universo incrível
seja ainda mais positiva!**

Índice

Cada mergulho é um flash!

Voltar

Oba! Todo mundo A-M-A postar nas redes sociais, participar das trends, se cadastrar em apps e sites incríveis, conhecer pessoas novas e tudo mais, certo? Estar na internet é “daora”, tem muita coisa de graça, mas não podemos marcar bobeira na hora de compartilhar nossos dados pessoais, publicar nossas fotos ou realizar cadastro em uma plataforma.

Suas informações pessoais valem muito! E tem muita gente com interesse naquilo que você disponibiliza no mundo on-line.

Pode ser uma novidade, uma foto que você achou linda, um vídeo engraçado que você fez, um áudio, um print de uma conversa ou qualquer outro conteúdo que você queira postar. Antes de fazê-lo, pergunte-se: isso pode prejudicar você ou mais alguém? Expõe alguma informação pessoal como endereço, nome de escola, empresa em que trabalha, e-mail, telefone, placa do carro? Identifica o local onde você está ou que costuma frequentar?

Postagens com muitos detalhes da rotina, com dados pessoais e até mesmo expondo a imagem de crianças e adolescentes podem ser usadas por estranhos para diferentes finalidades.

Para não ser um alvo fácil para oportunistas e criminosos virtuais, se liga nessas dicas:

Nas redes sociais, evite publicar endereços de lugares que frequenta, onde mora ou estuda.

Cuidado com as imagens que aparecem ao fundo das suas fotos e vídeos. Elas podem mostrar detalhes que você não gostaria que ficassem públicos.

Limite o acesso das pessoas que você não conhece àquilo que você posta na internet. Basta modificar suas configurações de privacidade e manter seu perfil aberto apenas para familiares e amigos.

g1

Veja mais: postagens em redes sociais foram utilizadas para planejar um assalto

Cuidado com o compartilhamento de senhas, nomes de usuário ou documentos. Recebeu alguma solicitação desses dados por telefone, WhatsApp ou e-mail? Confirme a veracidade por outros meios.

Ao realizar um cadastro em um app, site ou plataforma online, verifique se a empresa é confiável. Isso pode ser feito através de uma busca no seu navegador.

Viu uma notícia bombástica rolando por aí, mas ficou na dúvida se é real? Não compartilhe! Na seção 'Fato ou Fake' do G1 é feito um monitoramento diário de mensagens suspeitas que estão sendo compartilhadas nas redes sociais ou por apps de mensagens instantâneas, como o WhatsApp.

É uma cilada, Bino!

Voltar

Recebeu uma mensagem com aquela promoção imperdível, uma premiação de um sorteio que você nem lembra de ter participado ou uma oportunidade de emprego irrecusável?
Cuidado! Esse tipo de abordagem pode ser uma tentativa de golpe. Isso também pode vir acompanhado por um link, um pedido de contato, confirmação de dados pessoais, um formulário ou até mesmo um arquivo anexado. É assim que pessoas mal-intencionadas conseguem concretizar seus planos: a partir desse tipo de mensagem o atacante pode infectar o seu dispositivo com algum arquivo malicioso, roubar seus dados pessoais e até mesmo se passar por você.

Pintou uma dúvida? Não clique, não baixe arquivos anexados, não preencha formulários e não responda essas solicitações. Caso venha de uma pessoa conhecida, confirme por outro meio (telefone, WhatsApp, e-mail etc.).

Ah! E falando nisso... provavelmente você já deve ter ouvido falar dos "golpes do WhatsApp", certo?

Os mais comuns são o da clonagem de perfil e o do sequestro de conta. No primeiro, o criminoso se passa por você, utilizando nomes e fotos iguais aos seus, mas com número diferente. Sua conta continua normal no seu celular, mas eles se passam por você e pedem transferências, pagamentos e ajudas financeiras para seus familiares e amigos, que facilmente são enganados.

Para reduzir o risco de clonarem seu perfil, deixe sua foto e suas informações acessíveis apenas aos seus contatos.

Como fazer – No WhatsApp, abra: Configurações>>Conta>> Privacidade>>Foto de perfil>> Meus contatos.

No segundo, o criminoso obtém controle da sua conta de WhatsApp, que deixa de funcionar no seu celular.

Para se proteger desse tipo de abordagem, ative a confirmação de duas etapas. Já ouviu falar? Este item de segurança é fundamental. Com ele, para validar a sua conta será preciso o código de ativação (primeira etapa) e também um PIN (segunda etapa) que você cadastrará no próprio aplicativo.

Para ativar basta ir no WhatsApp, Abrir configurações>>Conta>> Confirmação em duas etapas>>Ativar>> Insira um PIN de 6 dígitos.

Vale lembrar:
jamais compartilhe o código de ativação ou o PIN com ninguém.

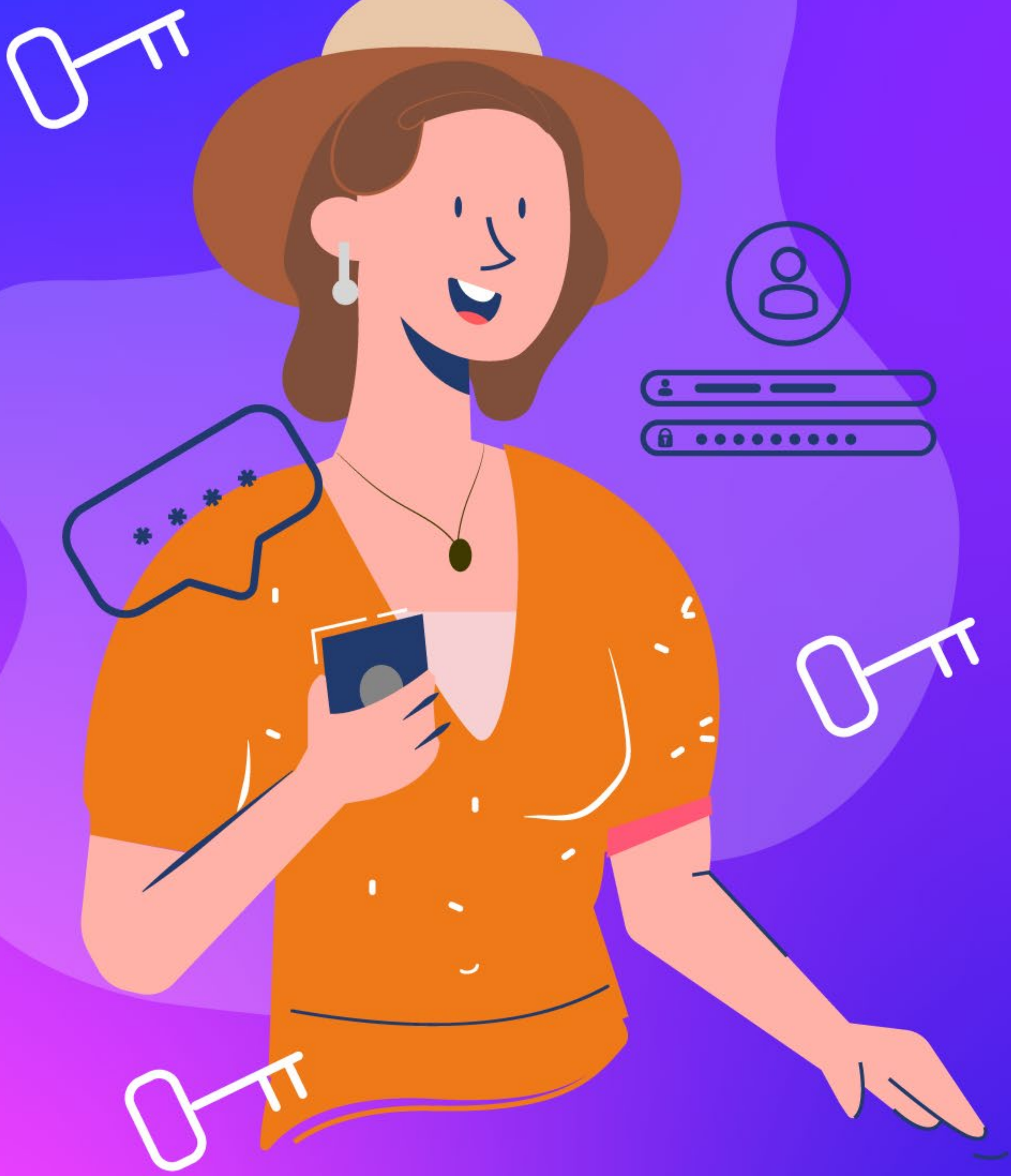
Proteção da caixa postal

E falando em código de ativação do WhatsApp, este é um dado valioso. Caso seja solicitado por qualquer pessoa, ele será enviado ao número vinculado à conta, por SMS ou ligação – podendo ir para a caixa postal se o aparelho estiver desligado ou se o chip não estiver no aparelho. Por isso é importante proteger a caixa postal com uma senha ou desabilitá-la junto à operadora (para saber mais contate o atendimento ao cliente).

g1

Saiba mais como se proteger e o que fazer se for vítima de golpes no WhatsApp.

Sou chique, bem.



Voltar

Mais do que chique, ser uma pessoa prevenida é “o must”, né?
Com a grande quantidade de serviços digitais, muitos usuários têm dificuldade em lidar com senhas e, quando isso acontece, normalmente escolhem senhas fáceis ou as repetem em diversos serviços.
Isso pode colocar a segurança das suas informações em risco.

Então se liga nas dicas para ter senhas fortes e mantê-las seguras:

Crie senhas com 10 caracteres ou mais usando, ao menos, uma letra maiúscula, uma minúscula, números e caracteres especiais.

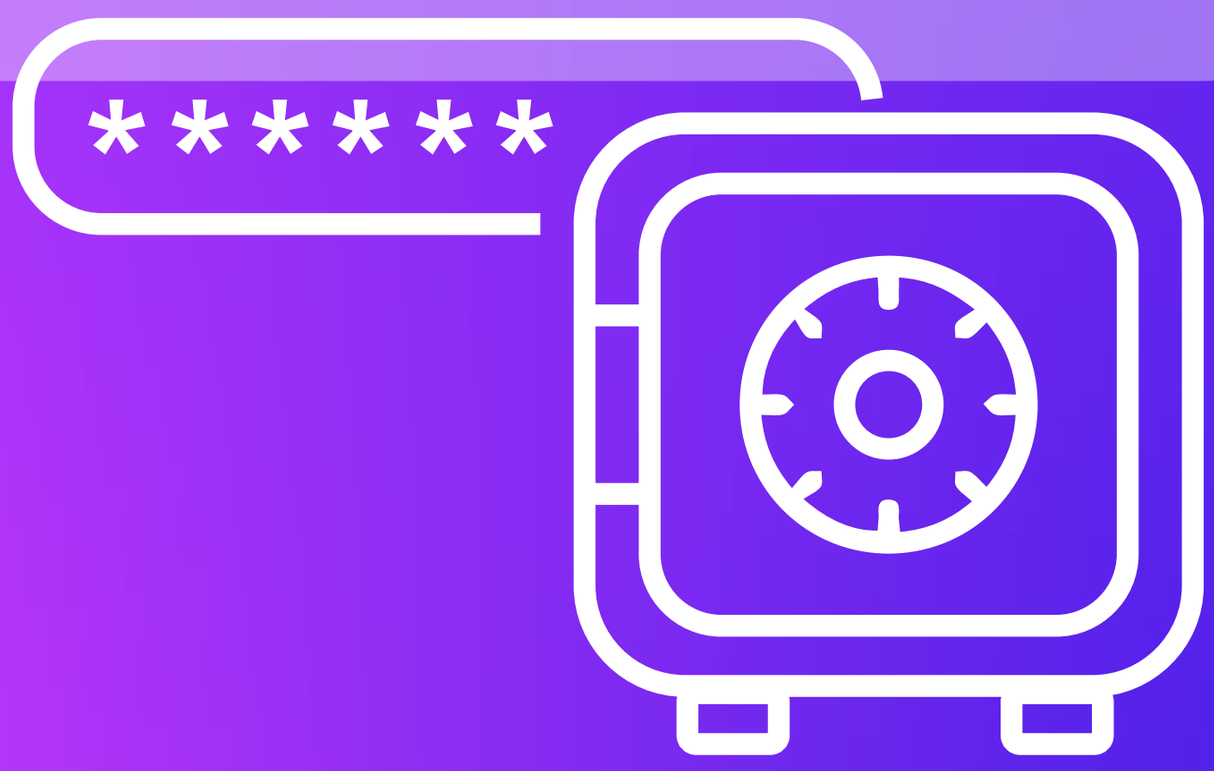
Usar nomes de pets, palavras comuns ou relacionadas a times de futebol, dados pessoais, nomes de parentes, sequências do teclado ou números de telefone pode tornar sua senha frágil.

Nunca armazene ou anote suas senhas em locais desprotegidos ou de fácil acesso, como post-its, planilhas, bloco de notas etc.

Fique atento ao digitar sua senha em locais públicos, alguém pode estar observando.

Evite compartilhar seus dados de acesso (login e senha).

Uma forma simples de criar e armazenar senhas é fazer uso de um gerenciador, também conhecido como “cofre de senhas”. Existem opções gratuitas e pagas no mercado.



Não abra mão do MFA (múltiplo fator de autenticação), que fornece uma verificação de identidade adicional ao acessar contas ou aplicativos, como a leitura de uma impressão digital ou a adição de um código recebido por aplicativo ou SMS.

O Mais Você dá a receita de uma senha segura.

Isso é felomenal!

Voltar

Fenomenal mesmo é ser “gente boa”, tratar os outros como você quer ser tratado, tanto on-line quanto na vida real. Às vezes precisamos pensar além das emoções e tomar as decisões certas ao escolher o que dizer e de que forma.

Antes de publicar, comentar ou compartilhar um conteúdo, analise se não é desmoralizante, humilhante ou até mesmo constrangedor. Não se deixe enganar, ofensa não é brincadeira!

Qualquer tipo de agressão virtual pode ser considerado crime previsto em lei. Conheça alguns tipos de agressões virtuais passíveis de punição:

Calúnia, injúria, racismo, difamação, assédio, ciberstalking, ciberbulliyng são alguns exemplos de práticas criminosas.

globo.com

Saiba Mais sobre: como agir em casos de crimes virtuais

Não é brinquedo não!

Voltar

Não dá mesmo para brincar quando o assunto é sério.

Está passando por alguma situação on-line ou offline que parece “sem solução”?
Converse sobre isso com alguém!
Quando não sabemos o que fazer, a melhor forma de resolver é pedindo ajuda.

Recebeu algum conteúdo impróprio? Denuncie! Dessa forma podemos ajudar as pessoas envolvidas, a comunidade e as próprias plataformas a bloquear esse tipo de ocorrência.

Presenciou ou foi vítima de alguma agressão virtual? Essas ocorrências podem ser denunciadas tanto pelo site da SaferNet quanto por uma delegacia especializada, veja aqui a lista.

Notícias relacionadas:

Crimes virtuais: saiba o que fazer caso esteja sofrendo ataques nas redes sociais

Cyberbullying: como identificar, impactos e consequências

Referências:

Cartilha SaferNet

Guia Google Seja Incrível na Internet

Internet com Responsa

Ministério dos Direitos Humanos e Cidadania

globo | Toda atitude conta – Segurança da informação

Safernet