SEGURANÇA NA INTERNET

PROTEGENDO SEUS DADOS E PRIVACIDADE

QUEM SOU EU?

DANIEL DAVID NUNES

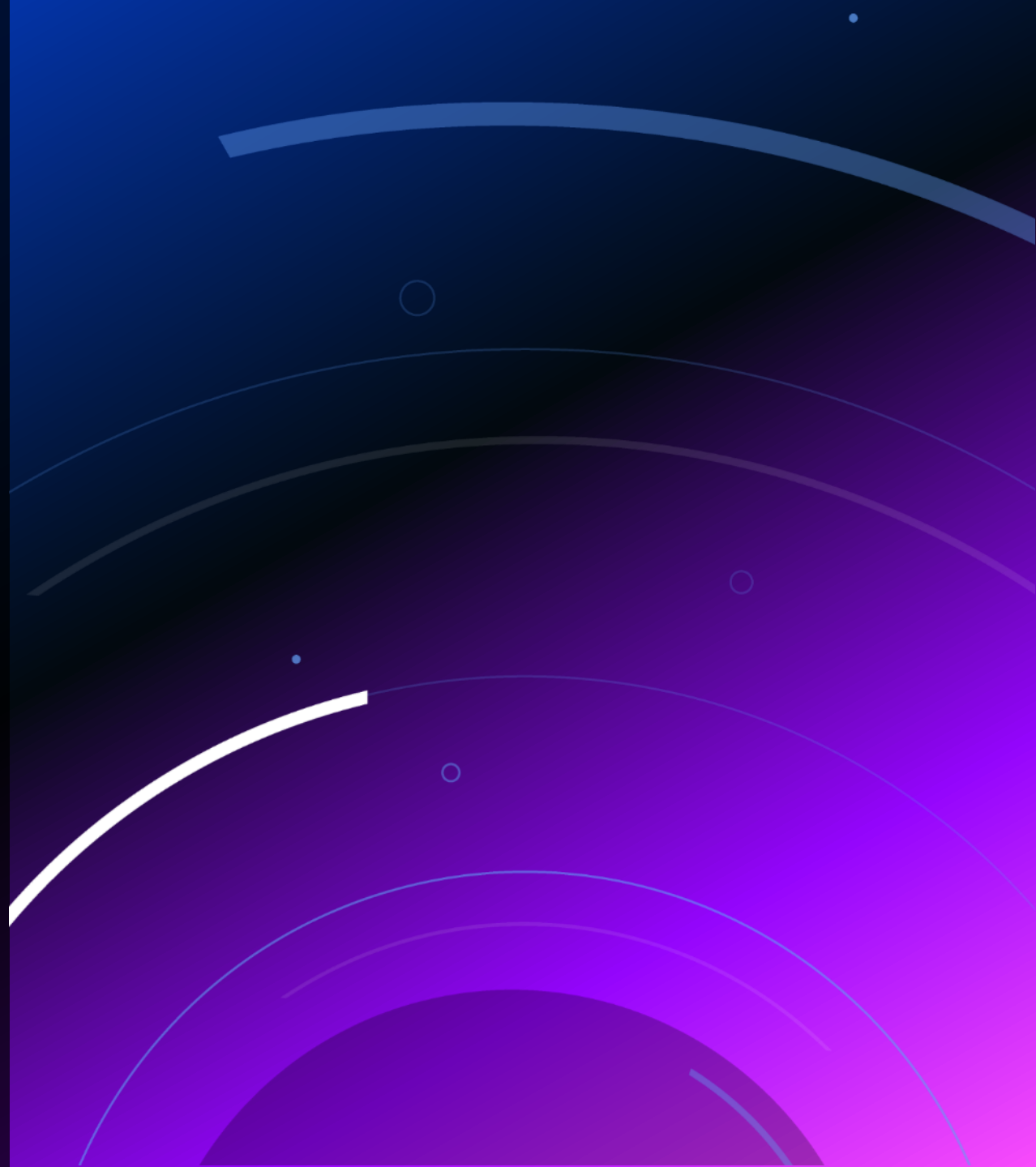
Gerente de Tecnologia da Informação na empresa Bookplay
Na empresa desde 2014
MBA em Segurança da Informação
Desenvolvedor Full Stack Sênior

TÓPICOS

Os dados e seus riscos

Técnicas de segurança

Dicas para o dia-a-dia

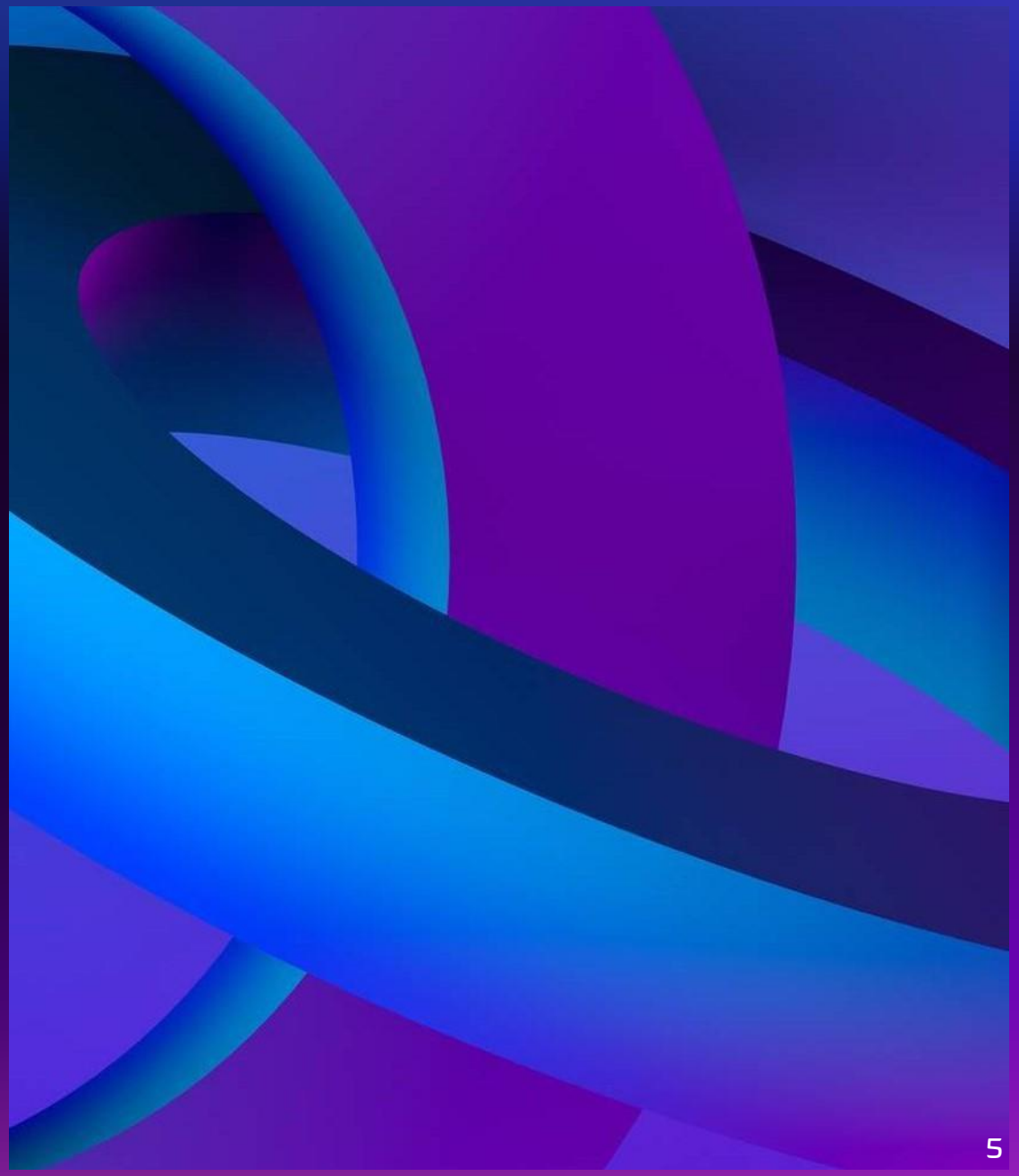


OS DADOS

E SEUS RISCOS

SUPEREXPOSIÇÃO

NAS REDES SOCIAIS



SUPEREXPOSIÇÃO NAS REDES SOCIAIS

As redes sociais são uma parte central da vida moderna, permitindo que as pessoas se conectem, compartilhem experiências e se mantenham informadas. No entanto, a superexposição nas redes sociais pode trazer riscos significativos à privacidade e à segurança pessoal. Vamos explorar essa questão mais detalhadamente...

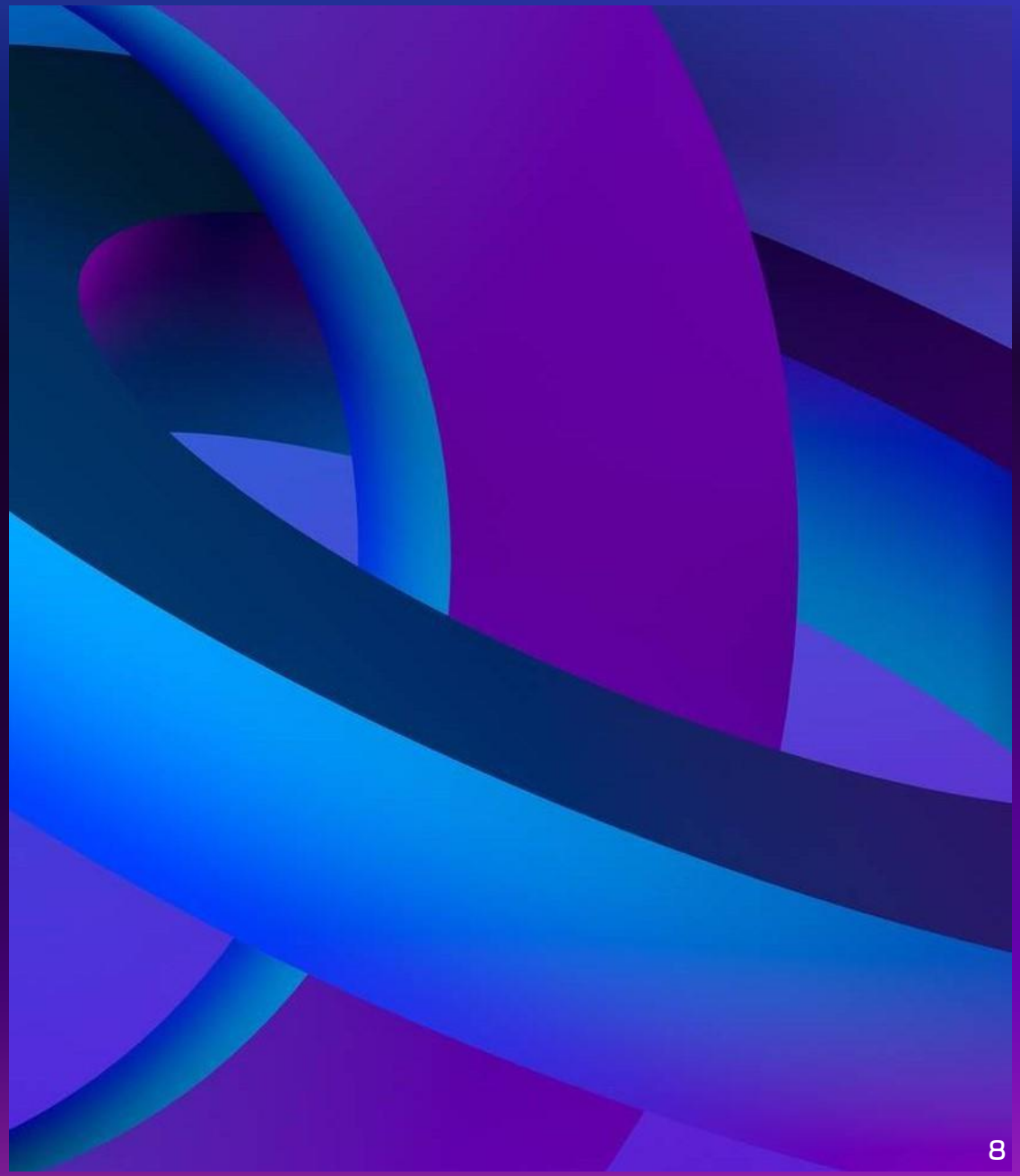
O QUE É SUPEREXPOSIÇÃO?

A superexposição ocorre quando uma pessoa compartilha excessivamente informações pessoais e detalhes da sua vida nas redes sociais. Isso pode incluir:

- **Localização geográfica em tempo real**
- **Detalhes sobre rotina diária**
- **Fotos e vídeos de momentos privados**
- **Informações financeiras ou de saúde**
- **Planos de viagem e ausência de casa**
- **Dados pessoais como endereço, telefone, documentos, datas importantes, etc**

E QUAIS OS RISCOS DE EXPORMOS NOSSOS

DADOS PESSOAIS?



UTILIZAÇÃO MALICIOSA DE DADOS PESSOAIS

Os dados pessoais podem ser explorados por criminosos de várias maneiras prejudiciais, como:

ROUBO DE IDENTIDADE

O roubo de identidade ocorre quando alguém utiliza os dados pessoais de outra pessoa sem autorização para cometer fraudes ou outros crimes. Exemplos incluem:

- **Abrir contas bancárias ou de crédito** em nome da vítima.
- **Solicitar empréstimos** utilizando as informações da vítima.
- **Fazer compras** com cartões de crédito obtidos fraudulentamente.
- **Realizar transações fraudulentas** que deixam a vítima responsável pelos débitos.

UTILIZAÇÃO MALICIOSA DE DADOS PESSOAIS

Os dados pessoais podem ser explorados por criminosos de várias maneiras prejudiciais, como:

FRAUDES FINANCEIRAS

Fraudes financeiras envolvem o uso de dados pessoais para obter ganho financeiro de maneira ilícita. Exemplos incluem:

- **Phishing:** Criminosos enviam e-mails ou mensagens fraudulentas que parecem vir de instituições legítimas para enganar as vítimas e coletar dados pessoais ou financeiros.
- **Scams de investimento:** Promessas de altos retornos em investimentos falsos utilizando as informações da vítima para persuadir a investir dinheiro.
- **Clonagem de cartão de crédito:** Utilizar os dados do cartão de crédito para realizar compras não autorizadas.

UTILIZAÇÃO MALICIOSA DE DADOS PESSOAIS

Os dados pessoais podem ser explorados por criminosos de várias maneiras prejudiciais, como:

GOLPES

Golpes utilizam dados pessoais para enganar as vítimas e levá-las a fazer algo contra seus próprios interesses. Exemplos incluem:

- **PIX no Whatsapp de um conhecido:** Criminosos entram em contato com um conhecido usando uma foto sua de alguma rede social e se passando por você pede dinheiro emprestado.
- **Golpe do falso sequestro:** Criminosos ligam para a vítima, alegando que sequestraram um ente querido, e exigem um resgate.
- **Falsificação de documentos:** Criar documentos falsos (como RG ou CNH) usando os dados pessoais da vítima para realizar atividades ilegais.
- **Fraude romântica:** Criminosos criam perfis falsos em sites de namoro para estabelecer um relacionamento com a vítima e, posteriormente, pedir dinheiro ou informações financeiras.

UTILIZAÇÃO MALICIOSA DE DADOS PESSOAIS

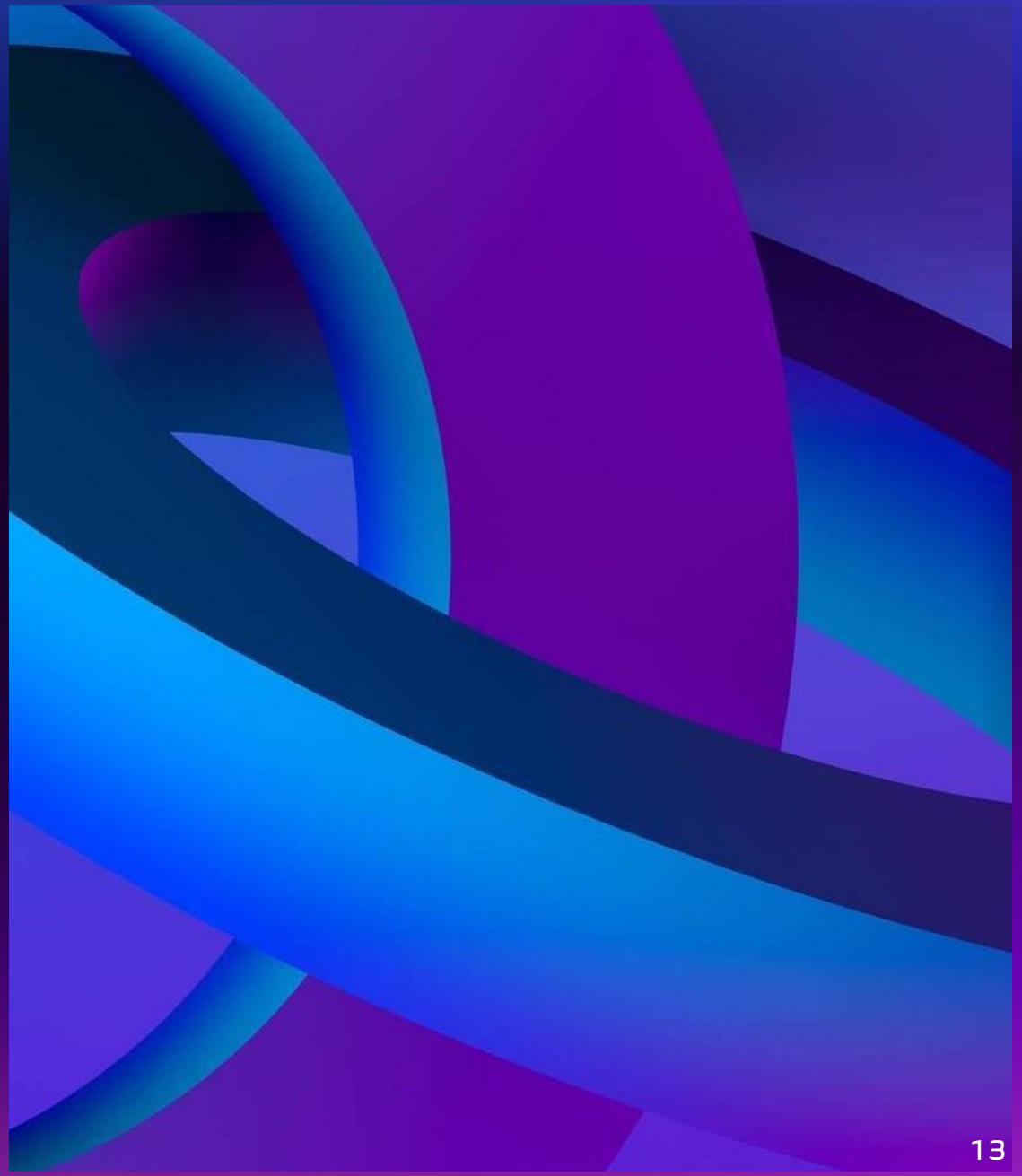
Os dados pessoais podem ser explorados por criminosos de várias maneiras prejudiciais, como:

ASSALTOS E SEQUESTROS

- **Check-ins Constantes:** Usar a funcionalidade de check-in para compartilhar sua localização exata pode informar a potenciais criminosos que você está longe de casa.
- **Segurança Pessoal:** Compartilhar a localização atual pode expor a pessoa a riscos físicos, como roubos ou sequestros. Criminosos podem usar essas informações para planejar atividades maliciosas.
- **Fotos de Crianças:** Compartilhar imagens de crianças com detalhes sobre suas escolas ou atividades pode colocá-las em risco.

PEDOFILIA:

UM CRIME SILENCIOSO



UM CRIME VIOLENTO E SILENCIOSO

Não é de hoje que a violência sexual contra crianças e adolescentes é um caso de emergência silencioso. Seja por qualquer canal que a pedofilia é praticada, as vítimas desse tipo de crime sofrem com ameaças e questionamentos sobre elas mesmas.

Dados da Ouvidoria Nacional dos Direitos Humanos apontam tendência de alta nos registros de denúncias de crimes sexuais contra crianças e adolescentes no Brasil em ambiente virtual. Apenas no primeiro semestre de 2022, mais de 78 mil denúncias foram registradas pela Ouvidoria. Deste total, 1,1 mil estão ligados a crimes de violência sexual que afetam a liberdade física ou psíquica da população infantojuvenil. Em comparação a 2020, os números do primeiro semestre do ano passado indicam alta de 97,6%. Em relação a 2021, o aumento foi de 80,1%.

Professora Kalinka Castelo Branco, do Departamento de Sistemas de Computação do Instituto de Ciências Matemáticas e de Computação (ICMC) da USP em São Carlos

Fonte: https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/#:~:text=N%C3%A3o%20%C3%A9%20de%20hoje%20que,e%20questionamentos%20sobre%20elas%20mesmas.

DEEPFAKE

Um dos agravantes nesse tipo de crime é que, muitas das vezes, não é possível identificar uma deepfake plenamente. No entanto, a professora Kalinka Castelo Branco, do Departamento de Sistemas de Computação do Instituto de Ciências Matemáticas e de Computação (ICMC) da USP em São Carlos, lista uma série de orientações básicas, como: ficar atento à movimentação de olhos e bocas e perceber se a pessoa pisca muito ou não pisca, se a boca se mexe ou não, se está mal enquadrada; atenção às emoções, quando é noticiado algo alegre, mas o rosto está triste ou o contrário; também verificar inconsistência na cor do rosto com o pescoço e colo; verificar o áudio e os ruídos; entre outras medidas.

Professora Kalinka Castelo Branco, do Departamento de Sistemas de Computação do Instituto de Ciências Matemáticas e de Computação (ICMC) da USP em São Carlos

Fonte: https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/#:~:text=N%C3%A3o%20%C3%A9%20de%20hoje%20que,e%20questionamentos%20sobre%20elas%20mesmas.

DEEPFAKE

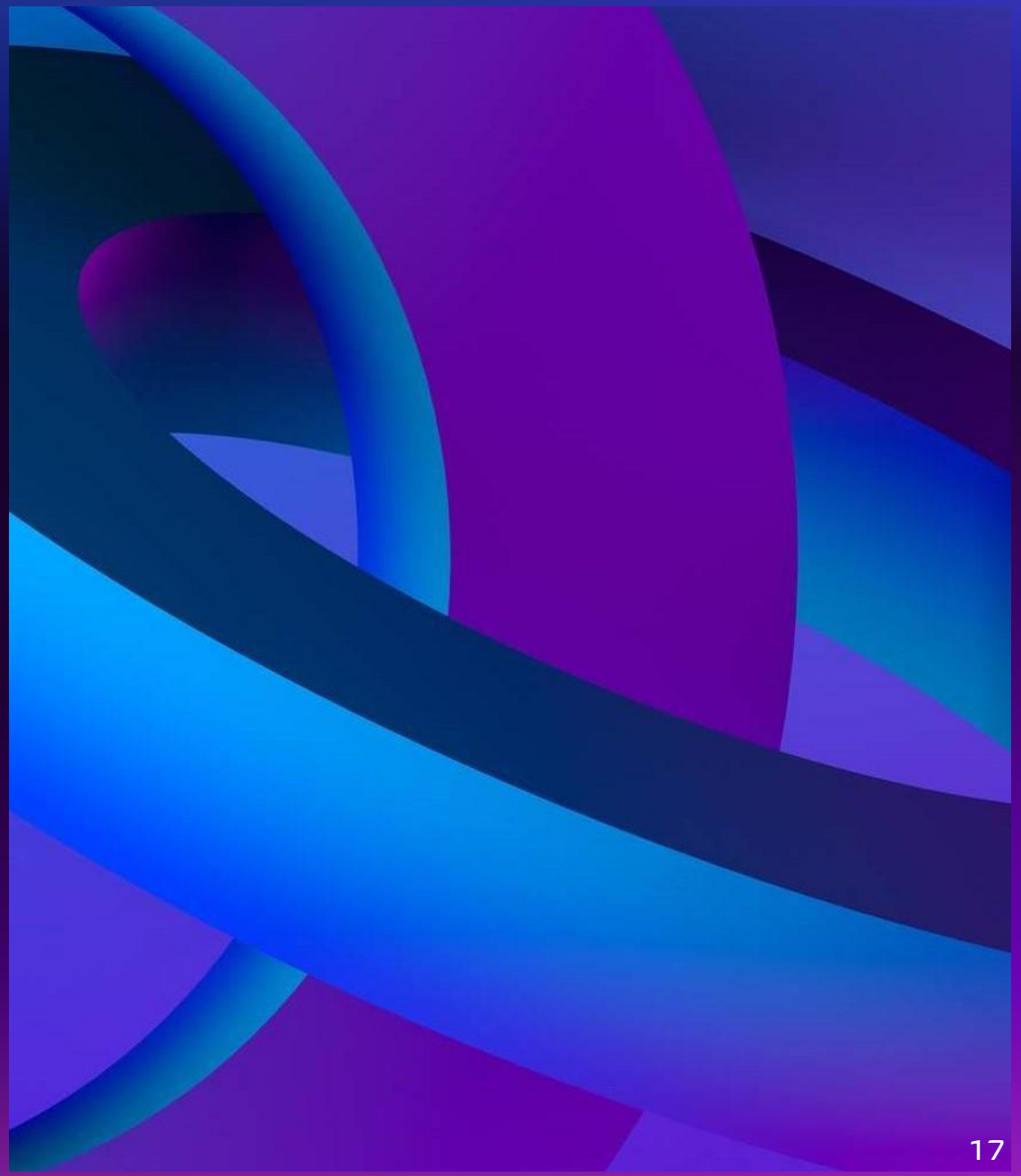
“Pedofilia é algo bastante grave e, sim, os criminosos virtuais estão sempre tentando se aproveitar da internet, do fato deles estarem por trás de uma câmera ou por trás de algum elemento”, alerta a professora. Ela adianta que uma forma de os pais protegerem seus filhos é não deixar que fiquem com o celular ou computador sozinhos sem a supervisão de um adulto, principalmente quando são pequenos.

Além disso, Kalinka pontua que os filhos têm sua individualidade, mas é responsabilidade dos pais ou responsáveis estarem sempre atentos. “Verifique o que eles estão acessando, as contas, o conteúdo e evite o computador no quarto onde eles podem acessar sozinhos sem que você esteja presente”, sugere.

Por fim, a especialista aponta ainda que um software de controle pode auxiliar nesse processo de verificação de conteúdo por parte dos responsáveis. “Eles auxiliam a verificar se a criança está tendo acesso a conteúdo que não deveria. Atitudes bastante simples de olhar e verificar com quem seu filho está falando na internet, o que ele está acessando, pode ajudar muito a evitar casos e problemas como de pedofilia virtual”, finaliza a professora.

USO INDEVIDO DE

IMAGEM NA INTERNET



USO INDEVIDO DE IMAGEM NA INTERNET

O uso indevido de imagens na internet é uma questão séria que afeta a privacidade e a dignidade das pessoas. Com o aumento do compartilhamento de fotos e vídeos nas redes sociais, esse problema tornou-se mais prevalente e preocupante.

É uma violação grave da privacidade e da dignidade humana. É essencial promover uma cultura de respeito e consentimento, educando as pessoas sobre os impactos e as responsabilidades associadas ao compartilhamento de imagens. Proteger a privacidade e a imagem das pessoas não é apenas uma questão legal, mas também ética e moral, fundamental para um ambiente digital seguro e respeitoso.

TIPOS DE USO INDEVIDO DE IMAGEM

- **Divulgação de Fotos Íntimas Sem Consentimento:** Também conhecido como "revenge porn" ou pornografia de vingança, ocorre quando alguém compartilha imagens ou vídeos íntimos de outra pessoa sem o seu consentimento. Isso pode causar imenso sofrimento emocional, vergonha e danos à reputação da vítima.
- **Cyberbullying**: Envolve o uso de imagens para intimidar, humilhar ou assediar alguém online. Isso pode incluir a postagem de fotos embaraçosas, a criação de memes depreciativos ou a manipulação de imagens para causar constrangimento.
- **Uso Não Autorizado em Publicidade**: Imagens de pessoas são usadas em anúncios ou promoções sem a devida autorização. Isso pode levar à exploração comercial da imagem da pessoa sem compensação ou reconhecimento.
- **Deepfakes**: Uso de tecnologia de inteligência artificial para criar vídeos ou imagens falsificadas que parecem reais. Deepfakes podem ser usados para enganar, difamar ou manipular a percepção pública sobre uma pessoa.

CONSEQUÊNCIAS DO USO INDEVIDO DE IMAGEM

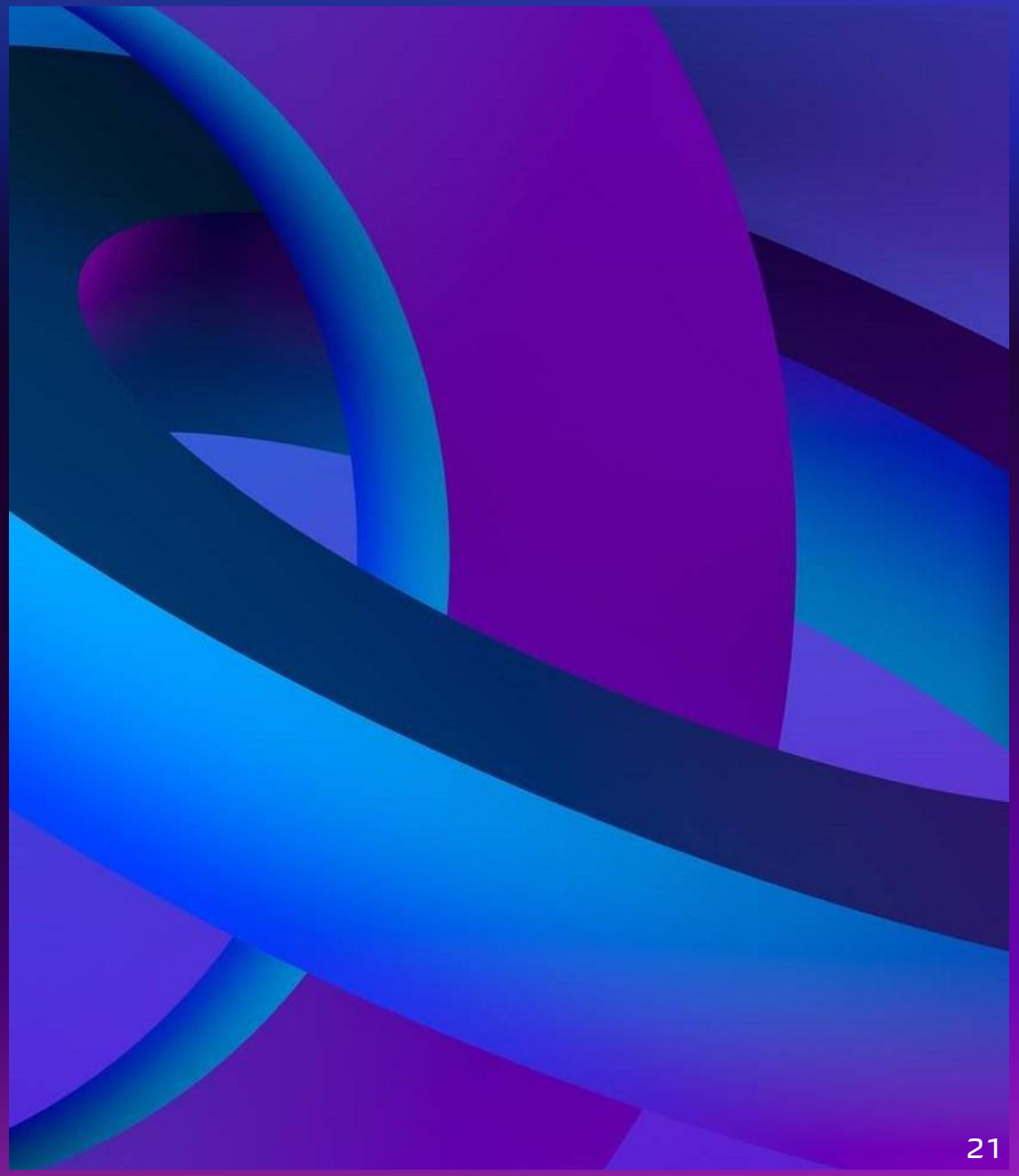
- **Danos Emocionais e Psicológicos:** As vítimas podem sofrer de ansiedade, depressão e perda de autoestima. A exposição pública de imagens íntimas ou embaraçosas pode causar traumas profundos.

- **Prejuízos à Reputação:** A reputação pessoal e profissional da vítima pode ser gravemente afetada, impactando suas relações sociais e oportunidades de emprego.

- **Consequências Legais:** Em muitos países, o uso indevido de imagens é considerado crime e pode resultar em processos judiciais, multas e até prisão para os criminosos.

EXEMPLOS

DE CASOS REAIS



CHANTAGEM COM FOTOS ÍNTIMAS DE INFLUENCIADORA DIGITAL (2018)

Uma influenciadora digital brasileira teve suas fotos íntimas roubadas por hackers que invadiram sua conta de e-mail. Os criminosos ameaçaram divulgar as fotos se ela não pagasse uma quantia em dinheiro. A influenciadora decidiu não ceder à chantagem e denunciou o caso às autoridades.

Impacto:

- Trauma emocional e stress significativo para a vítima.

CHANTAGEM A EMPRESÁRIO BRASILEIRO (2017)

Em 2017, um empresário brasileiro foi alvo de chantagem após hackers invadirem seu sistema de câmeras de segurança residencial. Os criminosos obtiveram imagens privadas e ameaçaram divulgá-las se o empresário não pagasse um resgate. O empresário procurou a polícia e o caso foi investigado, levando à identificação dos responsáveis.

Impacto:

- Sensação de insegurança e invasão de privacidade para a vítima.

REPORTAGENS SOBRE O PERIGO DA EXPOSIÇÃO EM REDES SOCIAIS

TÉCNICAS

DE SEGURANÇA

SENHAS FORTES

- Senhas fracas são mais fáceis de adivinhar ou quebrar usando ataques de força bruta ou dicionário. Hackers podem usar programas automatizados para tentar inúmeras combinações rapidamente.

- Senhas fortes ajudam a proteger suas contas contra acessos não autorizados, protegendo suas informações pessoais e dados financeiros.

- Usar senhas únicas para cada conta significa que, se uma senha for comprometida, suas outras contas permanecem seguras. Senhas reutilizadas facilitam ataques em cascata, onde um comprometimento leva a outros.

DICAS PARA CRIAR SENHAS SEGURAS E FÁCEIS DE LEMBRAR

- **Use Frases de Senha (Passphrases):** Combine várias palavras aleatórias para criar uma frase longa, como "CavaloAzulMelancia@1985". Isso aumenta o comprimento e a complexidade, mas pode ser mais fácil de lembrar.
- **Adicione Variabilidade:** Alterne entre letras maiúsculas e minúsculas, insira números e símbolos. Por exemplo, "G4t0s!C@Ch0rr0$&2021".
- **Evite Informações Pessoais:** Não use informações facilmente acessíveis ou adivinháveis, como seu nome, aniversário ou nomes de familiares e pets.
- **Utilize um Gerenciador de Senhas:** Gerenciadores de senhas podem criar e armazenar senhas fortes e únicas para cada uma de suas contas, como LastPass, 1Password ou Bitwarden. Isso elimina a necessidade de lembrar várias senhas complexas.
- **Adote um Método de Construção:** Use um método consistente para criar senhas. Por exemplo, pegue a primeira letra de cada palavra de uma frase memorável: "Minha casa é verde e bonita!" se torna "Mcev&b!123".
- **Atualize Regularmente:** Troque suas senhas periodicamente, especialmente para contas importantes ou se suspeitar que sua senha foi comprometida.

AUTENTICAÇÃO DE DOIS FATORES (2FA)

O que é Autenticação de Dois Fatores (2FA)?

- A Autenticação de Dois Fatores (2FA) é um método de segurança que exige duas formas de verificação antes de permitir o acesso a uma conta online.
- Os dois fatores geralmente incluem:
  - **Algo que você sabe:** Uma senha ou PIN.
  - **Algo que você tem:** Um dispositivo móvel para receber códigos ou uma chave de segurança.

Por que 2FA é Importante?

- **Aumenta a segurança:** Mesmo se a senha for comprometida, o acesso não é possível sem o segundo fator.
- **Proteção adicional:** Reduz significativamente o risco de acessos não autorizados, fraudes e roubos de identidade.

COMO A 2FA ADICIONA CAMADA EXTRA DE SEGURANÇA

Como Funciona a 2FA?

1. **Login Inicial:**
    1. Insira seu nome de usuário e senha.
2. **Segunda Verificação:**
    1. Receba um código via SMS, aplicativo de autenticação (como Google Authenticator ou Authy), ou utilize uma chave de segurança física.
3. **Acesso Permitido:**
    1. Insira o código recebido ou autentique com a chave física para completar o login.

Benefícios da 2FA:

- **Dificuldade para Hackers:** Ataques que obtêm apenas a senha são ineficazes sem o segundo fator.
- **Proteção em Casos de Phishing:** Mesmo que suas credenciais sejam roubadas, a segunda etapa impede o acesso.
- **Facilidade de Implementação:** Muitos serviços populares, como e-mail e redes sociais, já oferecem 2FA como uma opção de segurança.

CUIDADO COM LINKS E ANEXOS

Perigos de Clicar em Links:

- **Phishing:** Links maliciosos podem levar a páginas falsas que coletam informações pessoais.
- **Malware:** Clicar em links pode baixar malware que danifica seu dispositivo ou rouba dados.

Dicas de Segurança:

- **Verifique o Remetente:** Confirme se o e-mail é de uma fonte confiável antes de clicar.
- **Hover Antes de Clicar:** Passe o mouse sobre o link para ver a URL real antes de clicar.
- **Use um Antivírus Atualizado:** Proteja seu dispositivo com um antivírus robusto para identificar ameaças.

CUIDADO COM LINKS E ANEXOS

Perigos de Abrir Anexos

- **Ransomware:** Anexos podem conter software que bloqueia seus arquivos até que um resgate seja pago.
- **Vírus:** Abrir anexos pode infectar seu dispositivo com vírus que afetam seu desempenho.

Boas Práticas

- **Verificação de Segurança:** Use um programa de segurança para verificar anexos antes de abri-los.
- **Conscientização:** Treine sua equipe para identificar e-mails de phishing e anexos maliciosos.
- **Backup Regular:** Mantenha backups atualizados para proteger seus dados em caso de ataque.

CONFIGURAÇÕES DE PRIVACIDADE EM REDES SOCIAIS

Configurações de Privacidade

- **Controle de Visibilidade:** Defina quem pode ver suas publicações, fotos e informações pessoais.
- **Restrições de Compartilhamento:** Limite o acesso a suas postagens para amigos ou grupos específicos.
- **Segurança de Conta:** Ative autenticação de dois fatores (2FA) e revise as permissões de aplicativos conectados.

Cuidados com o que se Compartilha

- **Informações Pessoais:** Evite compartilhar dados sensíveis como endereços, números de telefone e informações financeiras.
- **Fotos e Vídeos:** Pense duas vezes antes de postar imagens íntimas ou comprometedoras.

CUIDADO COM O QUE SE COMPARTILHA ONLINE

Riscos de Compartilhamento Público

- **Roubo de Identidade:** Informações pessoais podem ser usadas para fraudes.
- **Reputação Online:** Postagens controversas podem afetar sua imagem profissional e pessoal.
- **Ataques Cibernéticos:** Dados expostos podem ser usados em golpes e phishing.

Boas Práticas

- **Revisão Regular:** Verifique e ajuste suas configurações de privacidade com frequência.
- **Consciência Digital:** Eduque-se e a outros sobre os riscos de compartilhamento inadequado.
- **Responsabilidade Social:** Ajude a proteger amigos e familiares, encorajando-os a adotar práticas seguras.

CUIDADO COM O QUE SE COMPARTILHA ONLINE

Riscos de Compartilhamento Público

- **Roubo de Identidade:** Informações pessoais podem ser usadas para fraudes.
- **Reputação Online:** Postagens controversas podem afetar sua imagem profissional e pessoal.
- **Ataques Cibernéticos:** Dados expostos podem ser usados em golpes e phishing.

Boas Práticas

- **Revisão Regular:** Verifique e ajuste suas configurações de privacidade com frequência.
- **Consciência Digital:** Eduque-se e a outros sobre os riscos de compartilhamento inadequado.
- **Responsabilidade Social:** Ajude a proteger amigos e familiares, encorajando-os a adotar práticas seguras.

CONCLUSÃO SOBRE

SEGURANÇA NA INTERNET

PROTEJA-SE ONLINE!

- **Dados Pessoais:** Mantenha suas informações pessoais seguras para evitar roubo de identidade e fraudes financeiras.
- **Pedofilia Online:** Eduque-se e eduque as crianças e os jovens sobre os perigos da internet para protegê-los de criminosos.
- **Uso Indevido de Imagem:** Respeite a privacidade dos outros e proteja-se contra o cyberbullying.
- **Exemplos de Casos Reais:** Aprenda com exemplos reais para entender os riscos e tomar medidas preventivas.
- **Senhas Fortes:** Use senhas longas e únicas para proteger suas contas online.
- **Autenticação de Dois Fatores (2FA):** Adicione uma camada extra de segurança às suas contas.
- **Cuidado com Links e Anexos:** Evite clicar em links suspeitos e abrir anexos não solicitados.
- **Privacidade em Redes Sociais:** Configure corretamente suas opções de privacidade e controle o que compartilha online.
- **Software de Segurança:** Use antivírus para proteger seus dispositivos contra ameaças cibernéticas.

MANTENHA-SE CONSCIENTE E INFORMADO!

- **Eduque-se e Eduque Outros:** Conscientize-se sobre as ameaças e práticas de segurança.
- **Monitoramento Regular:** Verifique e atualize regularmente suas configurações de segurança.
- **Denuncie Atividades Suspeitas:** Reporte e investigue qualquer atividade cibernética suspeita.

Juntos, podemos construir um ambiente online mais seguro!

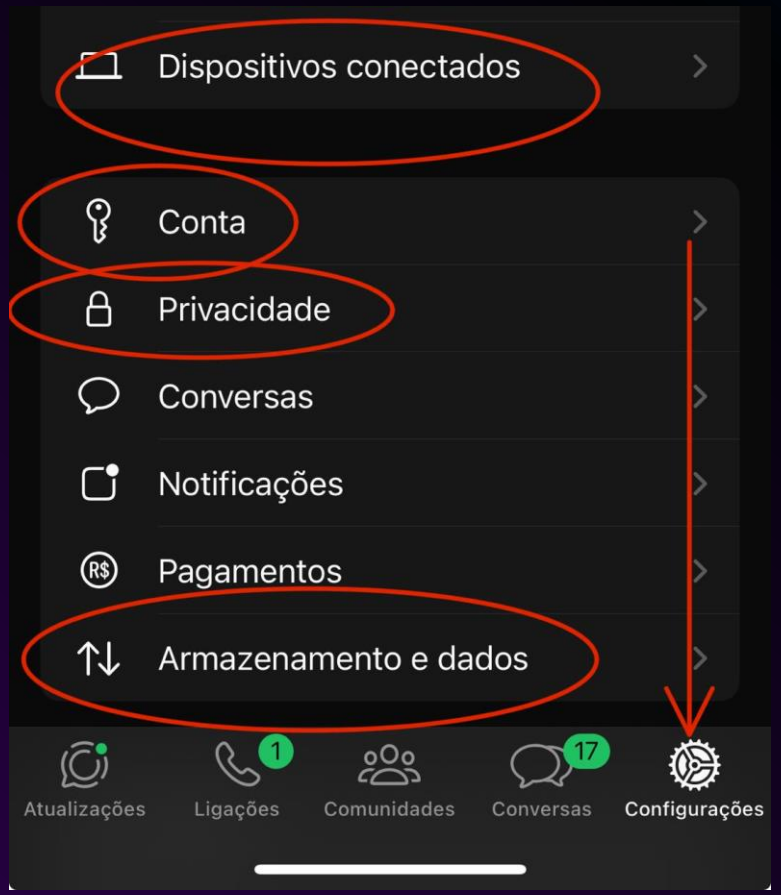
ALGUMAS DICAS DE SEGURANÇA

PARA O DIA-A-DIA

WHATSAPP

- **Não compartilhe dados pessoais e fotos:** Nas configurações de privavidade só permita que apenas seus contatos consigam acessar seus dados e status.
- **Desabilite download automático de mídias:** Nas configurações de armazenamento e dados desabilite os downloads automáticos, isso ajuda economizar espaço em seu celular e também que seja baixado algum arquivo malicioso.
- **Habilite a confirmação em duas etapas:** Nas configurações de conta habilite a Confirmação em duas etapas para evitar que acessem sua conta por outro aparelho caso consigam registrar.
- **Desconfie de contatos não conhecidos:** Tenha certeza de que a pessoa que está te chamando é ela mesma. Confirme com algum conhecido em comum o número do telefone.
- **PIX ou transações bancárias:** Se não estiver esperando uma solicitação de PIX desconfie até de contatos, sempre ligue para a pessoa pelo próprio Whatsapp para garantir que quem atenderá do outro lado é a pessoa de fato. Se ela não atender, denuncie e bloqueie o contato.
- **Whatsapp Web:** Evite abrir o Whatsapp Web no trabalho ou em computadores de outras pessoas, pois, se você esquecer aberto outras pessoas podem acessar suas mensagens que podem haver dados sensíveis seus como senhas ou mensagens, fotos e vídeos comprometedores.

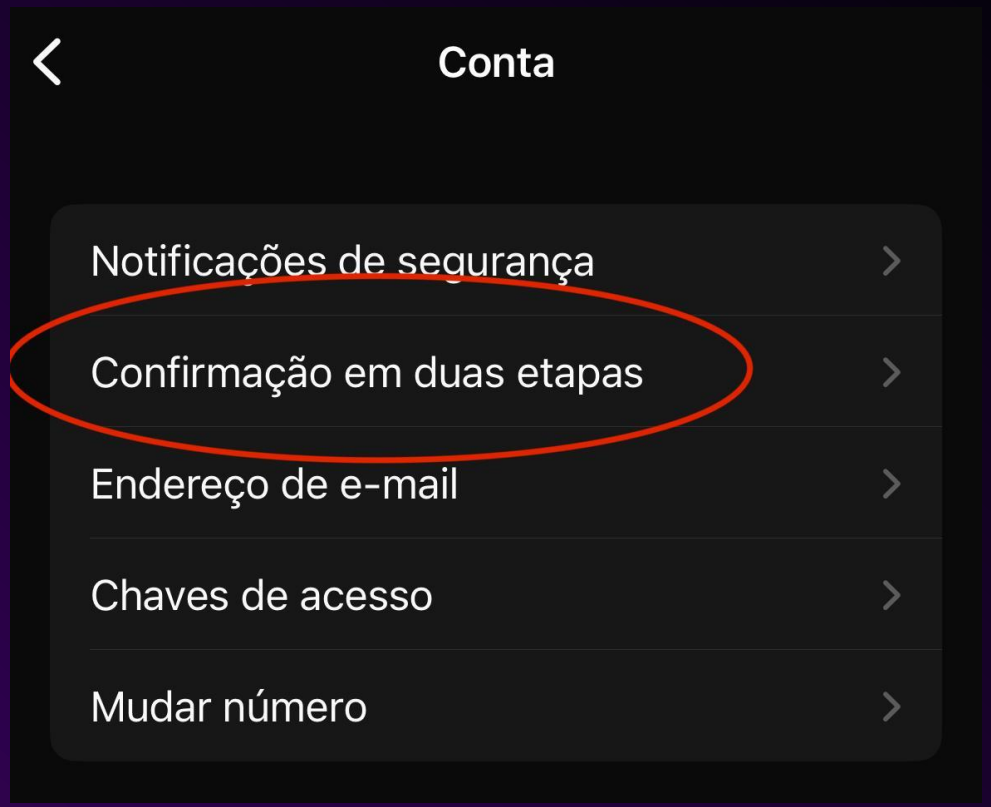
WHATSAPP - CONFIGURAÇÕES



WHATSAPP – CONFIGURAÇÕES > DISPOSITIVOS CONECTADOS

Desconecte de qualquer dispositivo que não seja seu.

WHATSAPP – CONFIGURAÇÕES > CONFIRMAÇÃO EM DUAS ETAPAS

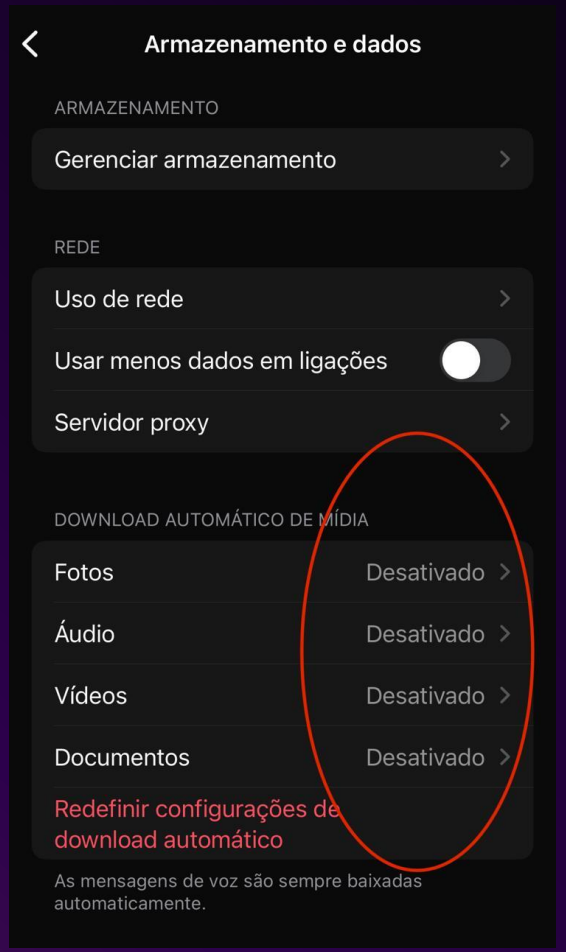


Ative a confirmação em duas etapas para ter uma segurança a mais e evitar que acessem seu Whatsapp.

WHATSAPP – CONFIGURAÇÕES > PRIVACIDADE

Permita que apenas seus contatos consigam acessar seus dados, foto de perfil e status.

WHATSAPP – CONFIGURAÇÕES > ARMAZENAMENTO E DADOS



Não faça downloads automáticos, assim você economiza espaço no celular e evita baixar algo malicioso que infecte seu celular.

SMS

- **SMS de compra no cartão de crédito:** Se você não fez uma compra e chegou a notificação, JAMAIS entre em contato com o telefone que o SMS pede para ligar ou clique em links. Acesse o site ou aplicativo do seu cartão de crédito e verifique se a compra ocorreu de fato e caso seja necessário entre em contato com o canal oficial do site da instituição financeira.

E-MAIL

- **Confirme a Autenticidade:** Certifique-se de que o e-mail é de um remetente confiável e conhecido. Verifique o endereço de e-mail para garantir que não haja pequenas alterações ou erros que indiquem um remetente falso.
- **Não Confie em E-mails Inesperados:** Se você não estava esperando um e-mail, especialmente de instituições financeiras ou serviços online, seja cauteloso ao abri-lo.
- **Assuntos Sensacionalistas:** Assuntos que criam um senso de urgência ou pânico, como “Sua conta será suspensa!” ou “Você ganhou um prêmio!”, são frequentemente usados em e-mails maliciosos.
- **Evite Links Suspeitos:** Passe o mouse sobre os links (sem clicar) para ver o URL real. Se o link parece suspeito ou não corresponde ao site oficial, não clique.
- **Anexos Perigosos:** Não abra anexos de e-mails desconhecidos ou inesperados. Eles podem conter malware ou vírus. Se o anexo parecer suspeito, exclua o e-mail imediatamente.
- **Erros de Linguagem:** E-mails maliciosos frequentemente contêm erros ortográficos e gramaticais, o que pode ser um indicativo de fraude.

E-MAIL COM REMETENTE SUSPEITO

CEMONTIM - Central de Monitoramento Infracional Móvel - Infração: 54527

De DENATRAN 22 Data Ter. 09:28

infracional-movel5360@b0mbeiros2024i.agencia-estatal.com

CEMONTIM - Central de Monitoramento Infracional Móvel

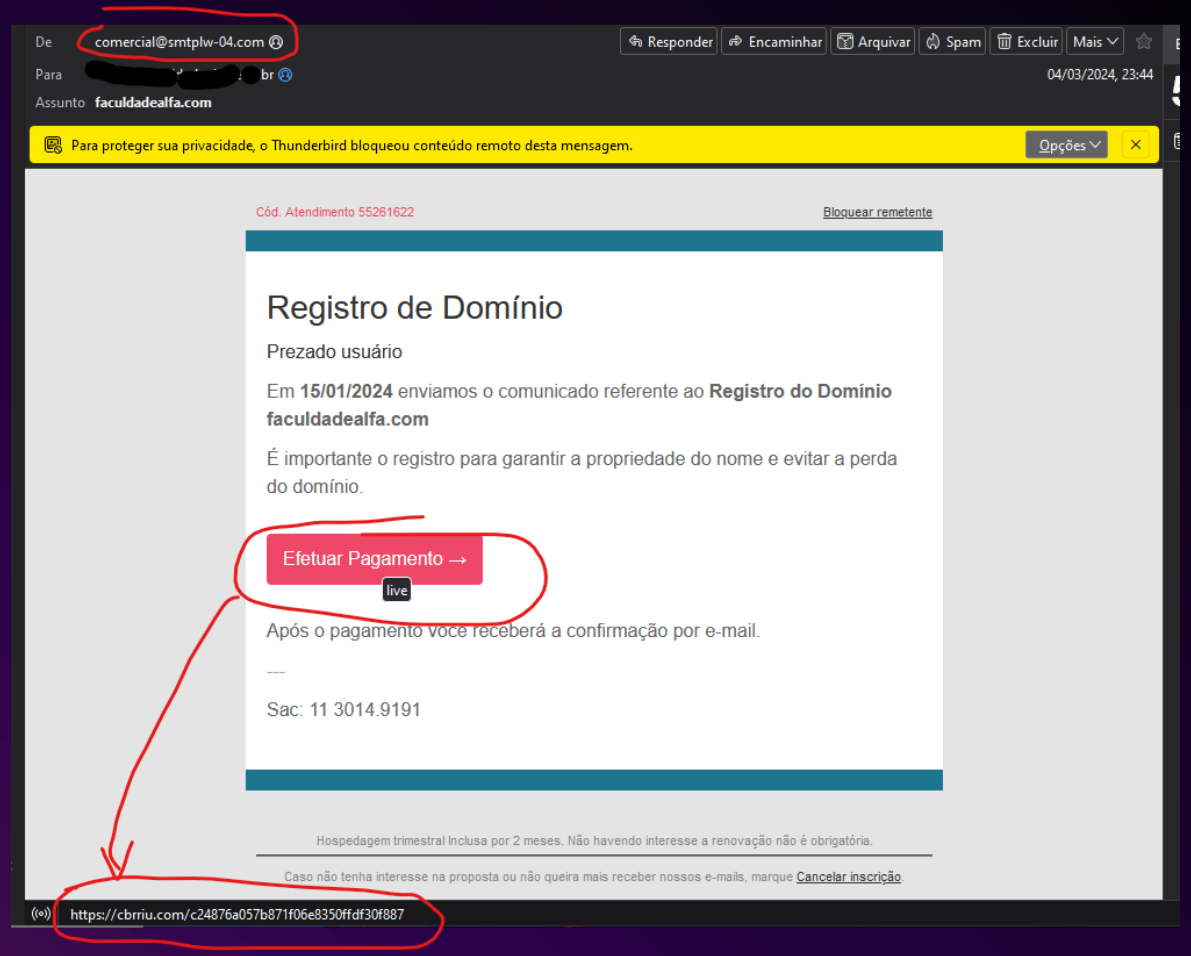
DENATRAN - Departamento Nacional de Trânsito

ADM/NMEP:	5549	**Autuação MTB/08:** Abrir Multa	
Data da Emissão:	28/05/2024	**Verificador:**	W0vGe2
Latitude/Long:	Anexo	**Expedição:**	Drone/688226

E-mail enviado automaticamente, favor não responder.
Em caso de dúvidas, favor entrar em contato pelos canais de comunicação.

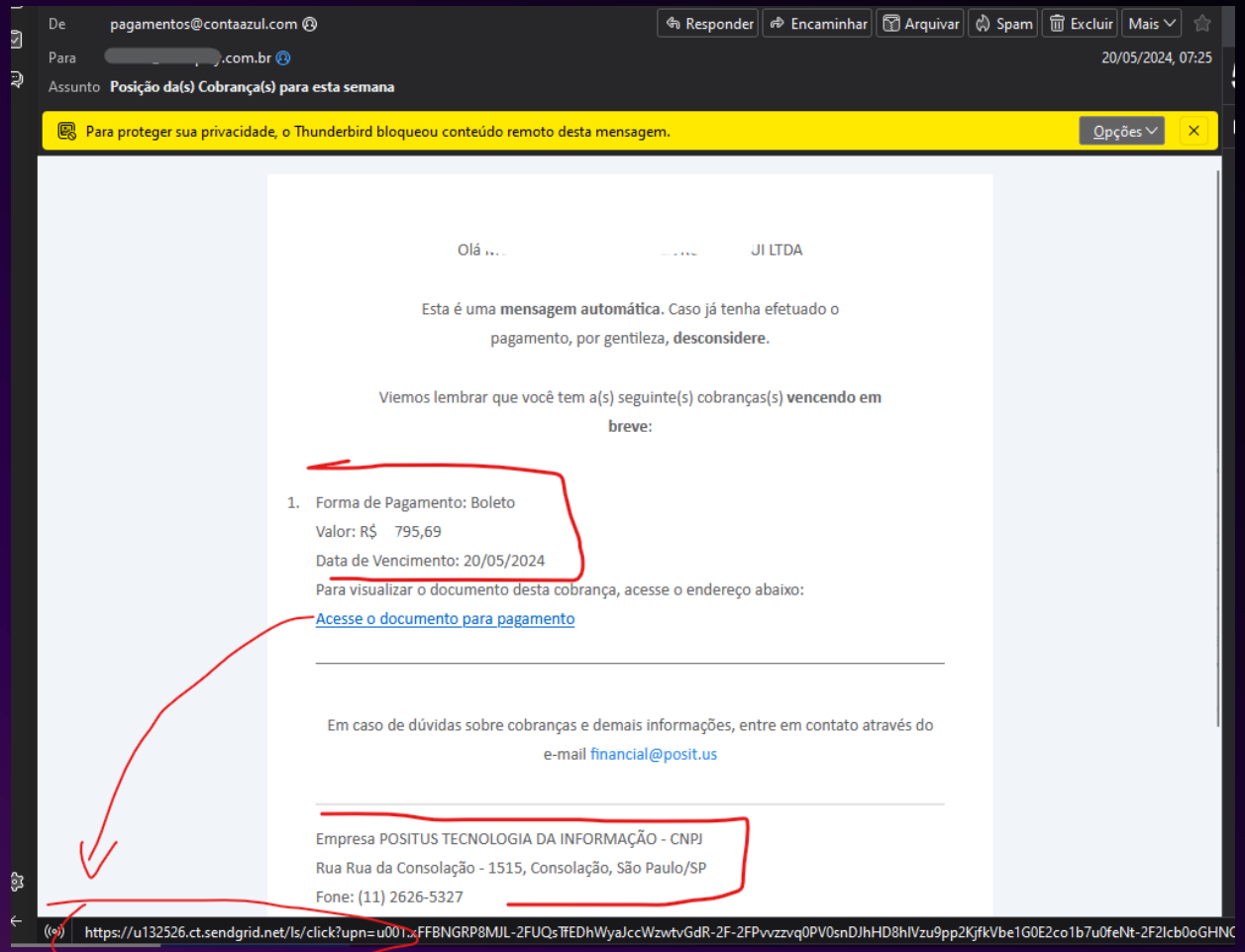
E-mail com domínios sem “.com.br” no final são suspeitos por serem internacionais e neste caso o e-mail veio como infracional-movel5360@b0mbeiros2024i.agencia-estatal.com tudo para tentar enganar, mas certamente é um golpe.

E-MAIL COM ENDEREÇO E LINK SUSPEITOS



Não esperava este e-mail e o endereço de e-mail do remetente é muito estranho e não é “.com.br”, e quando vamos para o link para Efetuar Pagamento ele aponta para um link mais estranho ainda que nem é o mesmo do endereço de e-mail. ESTE E-MAIL É CERTAMENTE UM GOLPE.

E-MAIL COM LINK SUSPEITO, PORÉM, VERDADEIRO



Apesar de ter um link enorme sem “.com.br” ao final, o que o deixa muito suspeito, ao confirmar que veio em nome da empresa, o credor do boleto bate com a data de vencimento e valor, confirma-se que é um e-mail real mesmo e este link, neste caso, é assim por ser enviado por campanhas de e-mail marketing, então pode-se clicar neste link que não haverá problemas.

WI-FI PÚBLICA

- **Não Acesse Contas Bancárias ou Compre Online:** Evite realizar transações financeiras ou acessar contas sensíveis enquanto estiver em redes Wi-Fi públicas.
- **Confirme a Autenticidade:** Verifique o nome da rede Wi-Fi com o estabelecimento para garantir que você está se conectando à rede legítima.
- **Camada Extra de Segurança:** Ative a autenticação de dois fatores nas suas contas importantes para uma proteção adicional.
- **Não informe seus dados reais no cadastro da rede:** Muitas redes grátis em estabelecimentos pedem para você preencher com seus dados como Nome completo, CPF, Data de Nascimento e telefone. Se for possível, não informe nenhum dado real, pois, estes dados certamente serão vendidos para mailings de vendas ou grupos de golpistas.

QR-CODES EM VIAS PÚBLICAS

- **Confirme a Legitimidade:** Certifique-se de que o QR code está sendo exibido por uma fonte confiável, como um anúncio oficial ou um estabelecimento conhecido.
- **Analise o Link:** Após escanear o QR code, verifique o URL ao qual você está sendo redirecionado antes de clicar. Desconfie de URLs abreviados ou estranhos.
- **Evite Transações Financeiras:** Não utilize QR codes em vias públicas para realizar pagamentos ou fornecer informações financeiras sem confirmação adicional da legitimidade.
- **Ambientes Confiáveis:** Não escaneie QR codes encontrados em locais suspeitos, como em postes de luz ou paredes de edifícios abandonados.
- **Desconfie de QR Codes Sobrepostos::** Verifique se o QR code não foi colado sobre outro código ou se não parece alterado. QR codes adulterados são frequentemente usados para redirecionar usuários para sites maliciosos.

CARTÃO DE CRÉDITO EM SITES

Compre em Sites Confiáveis:

- **Verifique a Reputação:** Certifique-se de que o site é confiável e tem boa reputação. Procure avaliações e feedback de outros usuários.
- **Certificado de Segurança:** Verifique se o site utiliza HTTPS na barra de endereço, indicando uma conexão segura.

Use Cartões Virtuais:

- **Cartões Temporários:** Muitos bancos oferecem cartões virtuais ou temporários para compras online, limitando o valor e a validade para reduzir riscos.

Habilite Alertas de Transações:

- **Monitoramento:** Ative notificações de transações por SMS ou e-mail para ser informado imediatamente sobre qualquer uso do seu cartão.

CARTÃO DE CRÉDITO EM SITES

Não Salve Dados do Cartão:

- **Armazenamento Seguro:** Evite salvar os dados do seu cartão de crédito em sites. Digite as informações manualmente em cada compra para evitar que sejam comprometidas.

Use Serviços de Pagamento Seguros:

- **Intermediários Confiáveis:** Utilize serviços de pagamento como PayPal, Apple Pay, Google Wallet ou outras opções seguras que oferecem proteção adicional para as transações.

Controle de Crédito:

- **Limite de Crédito:** Considere definir um limite de crédito mais baixo para compras online, reduzindo o impacto em caso de fraude.

Atenção a Ofertas Muito Boas:

- **Desconfie de Ofertas Incríveis:** Se uma oferta parece boa demais para ser verdade, pode ser um golpe. Verifique a legitimidade do site e da oferta.

PAGAMENTOS DE BOLETOS

Verifique a Autenticidade:

- **Confirme o Destinatário:** Verifique se o beneficiário do boleto corresponde à empresa ou serviço correto.
- **Linha Digitável:** Confira a linha digitável e os valores com os dados fornecidos pelo credor.

Desconfie de Ofertas e Descontos:

- **Boletos com Desconto:** Boletos que oferecem descontos não anunciados ou valores diferentes devem ser verificados com a empresa antes do pagamento.

Atenção aos Detalhes:

- **Valores e Datas:** Verifique valores, datas de vencimento e outras informações para garantir que o boleto é autêntico.
- **Comprovante de Pagamento:** Guarde sempre o comprovante de pagamento para futuras conferências.

POSTAGENS EM REDES SOCIAIS

- **Privacidade nas Redes Sociais:** Ajuste as configurações de privacidade para controlar quem pode ver suas postagens. Configure suas contas para que apenas amigos ou seguidores selecionados possam ver suas fotos.
- **Dados Sensíveis:** Não poste fotos que revelem informações pessoais, como endereço, número de telefone, documentos de identidade ou detalhes financeiros.
- **Localização:** Desative a geolocalização nas suas fotos para evitar que sua localização seja divulgada. Isso pode ser feito nas configurações da câmera do seu smartphone ou nas configurações de privacidade da rede social.
- **Impacto a Longo Prazo:** Considere as implicações futuras antes de postar uma foto. Lembre-se de que, uma vez na internet, a imagem pode ser difícil de remover completamente.

POSTAGENS EM REDES SOCIAIS - CRIANÇAS

- **Segurança Infantil:** Evite postar fotos de crianças que revelem detalhes sobre onde elas moram, estudam ou participam de atividades. Jamais poste fotos de seus filhos tomando banho, mesmo que bebês em banheiras, chuveiros, de roupa de banho numa praia, ou fotos que revelem o corpo de seu filho, pois, pedófilos se aproveitam de fotos assim para compartilharem em seus grupos e nunca se sabe se há algum em seu circulo de amizades ou familiar. Mantenha a privacidade e a segurança das crianças em mente.

- **Impacto a Longo Prazo:** Considere as implicações futuras antes de postar uma foto. Lembre-se de que, uma vez na internet, a imagem pode ser difícil de remover completamente e seu filho, futuramente, pode sofrer com uma exposição causada por você no passado.

MONITORE O QUE SEU FILHO ACESSA OU CONVERSA NO CELULAR – PARTE 1

Utilize Aplicativos de Controle Parental:

- **Aplicativos de Controle:** Existem diversos aplicativos de controle parental que permitem monitorar o uso do celular, como Qustodio, Norton Family, e Bark. Esses aplicativos oferecem recursos como bloqueio de sites, relatórios de atividades e monitoramento de mensagens.
- **Configurações do Sistema:** Muitos sistemas operacionais de smartphones, como iOS e Android, possuem recursos embutidos de controle parental. No iOS, use o "Tempo de Uso" e, no Android, utilize o "Family Link".

Configure Restrições de Conteúdo:

- **Restrições de Apps:** Defina restrições para baixar e usar aplicativos. No iOS, isso pode ser feito nas configurações de "Tempo de Uso". No Android, use o "Family Link" para definir limites e restrições.
- **Filtragem de Conteúdo:** Ative a filtragem de conteúdo nos navegadores e aplicativos para evitar que seu filho acesse conteúdo inadequado.

MONITORE O QUE SEU FILHO ACESSA OU CONVERSA NO CELULAR – PARTE 2

Monitore as Redes Sociais:

- **Configurações de Privacidade:** Configure as opções de privacidade nas redes sociais que seu filho usa, como Facebook, Instagram e TikTok, para limitar quem pode ver suas postagens e interagir com ele.
- **Acesso às Contas:** Se possível, tenha acesso às contas de redes sociais do seu filho para monitorar suas atividades e interações.

Estabeleça Regras Claras:

- **Regras de Uso:** Defina regras claras sobre o uso do celular, incluindo limites de tempo e horários específicos para uso.
- **Discussão Aberta:** Converse com seu filho sobre os riscos online e a importância de manter a privacidade e a segurança.

MONITORE O QUE SEU FILHO ACESSA OU CONVERSA NO CELULAR – PARTE 3

Verifique o Histórico de Navegação:

- **Navegadores:** Regularmente verifique o histórico de navegação nos navegadores usados por seu filho para monitorar os sites que ele acessa.
- **Limpeza de Histórico:** Esteja atento à limpeza frequente do histórico, que pode indicar tentativas de ocultar atividades.

Utilize Funcionalidades de Monitoramento em Mensageiros:

- **Aplicativos de Mensagens:** Alguns aplicativos de controle parental podem monitorar mensagens em apps como WhatsApp e SMS. Certifique-se de escolher um aplicativo que suporte os mensageiros que seu filho utiliza.

MONITORE O QUE SEU FILHO ACESSA OU CONVERSA NO CELULAR – PARTE 4

Controle de Compras e Downloads:

- **Compras In-App:** Ative controles de compra e exigência de senha para qualquer compra de aplicativos ou itens dentro de apps.
- **Downloads:** Monitore e aprove manualmente os downloads de novos aplicativos para garantir que eles sejam apropriados.

Eduque sobre Segurança Online:

- **Conscientização:** Ensine seu filho sobre os perigos de compartilhar informações pessoais online e como reconhecer e evitar interações suspeitas.
- **Comportamento Online:** Discuta a importância de ser respeitoso e cuidadoso ao interagir com outras pessoas online.

MONITORE O QUE SEU FILHO ACESSA OU CONVERSA NO CELULAR – PARTE 5

Use a Função de Relatórios e Alertas:

- **Relatórios de Atividade:** Configure os aplicativos de controle parental para enviar relatórios regulares sobre as atividades online do seu filho.
- **Alertas em Tempo Real:** Ative alertas para atividades suspeitas ou tentativas de acessar conteúdo restrito.

Mantenha uma Comunicação Aberta:

- **Diálogo Contínuo:** Mantenha uma comunicação aberta e honesta com seu filho sobre suas atividades online. Estabeleça um ambiente em que ele se sinta à vontade para falar sobre suas experiências e preocupações na internet.

APLICATIVOS DE CONTROLE PARENTAL

Existem vários aplicativos disponíveis no mercado e maioria tem as seguintes características:

- Monitoramento de atividade na web
- Controle de tempo de tela
- Rastreamento de localização
- Monitoramento de chamadas e mensagens
- Relatórios detalhados

Plataformas: iOS, Android

Os mais conhecidos são:
Qustodio, Norton Family, Bark, Family Link (Google), Kaspersky Safe Kids, Net Nanny, Mobicip, OurPact, MMGuardian, ESET Parental Control

Baixe agora as dicas para o dia-a-dia

https://mund.digital/rh/seguranca_na_internet-dicas.pdf

BOM, ENTÃO...

É ISSO AÍ!

OBRIGADO

Daniel David Nunes

@daniel.davidnunes