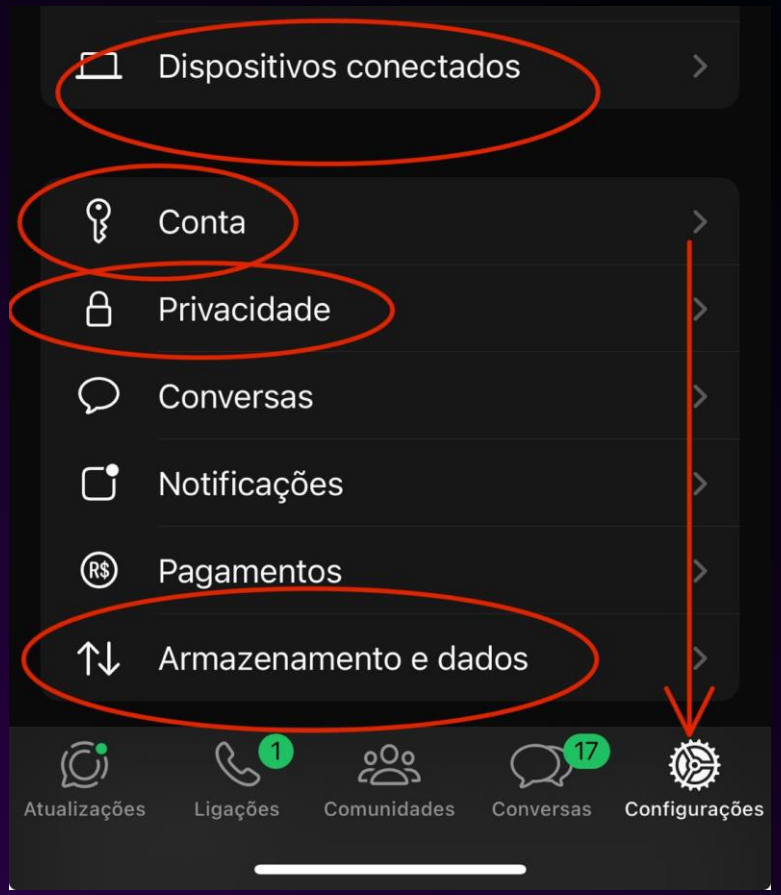
ALGUMAS DICAS DE SEGURANÇA

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.

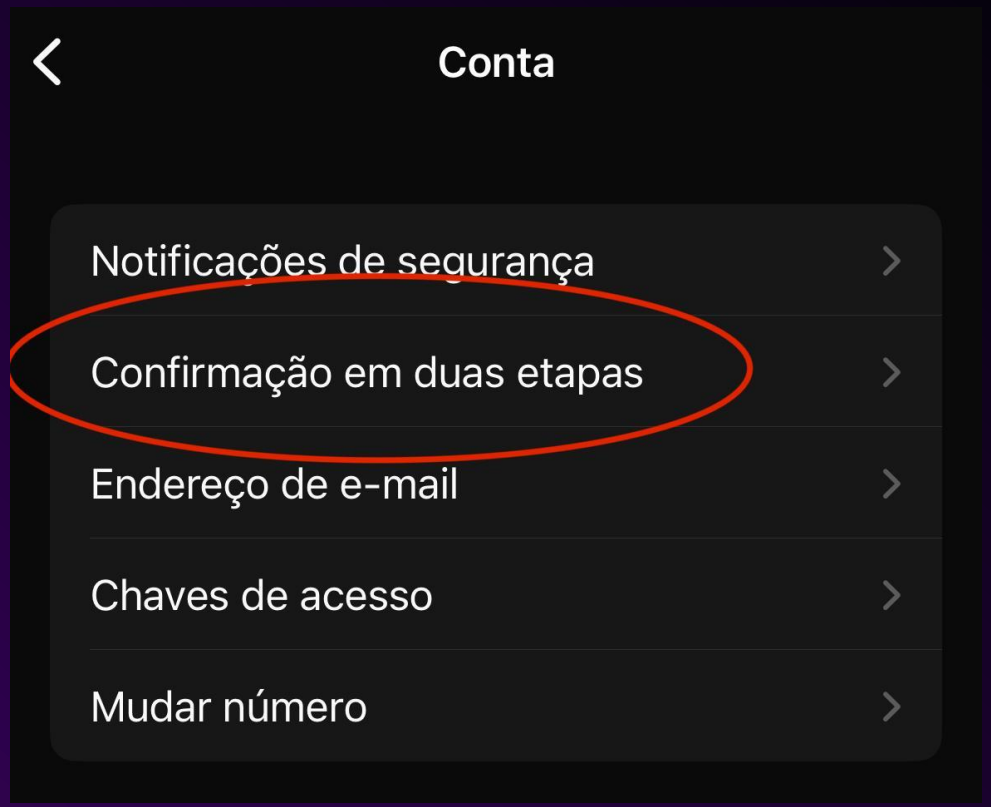
WHATSAPP - CONFIGURAÇÕES



WHATSAPP – CONFIGURAÇÕES > DISPOSITIVOS CONECTADOS

Desconecte de qualquer dispositivo que não seja seu.

WHATSAPP – CONFIGURAÇÕES > CONFIRMAÇÃO EM DUAS ETAPAS

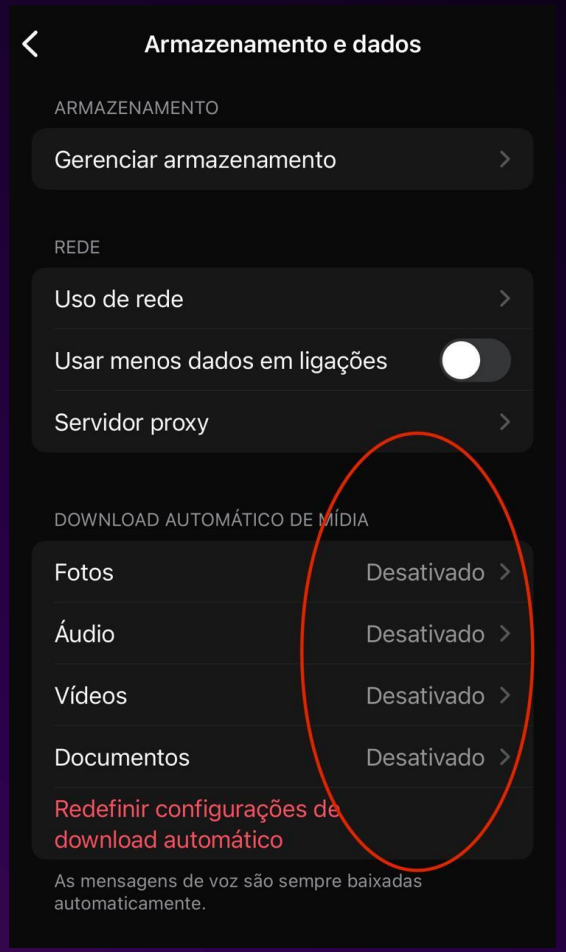


Ative a confirmação em duas etapas para ter uma segurança a mais e evitar que acessem seu Whatsapp.

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

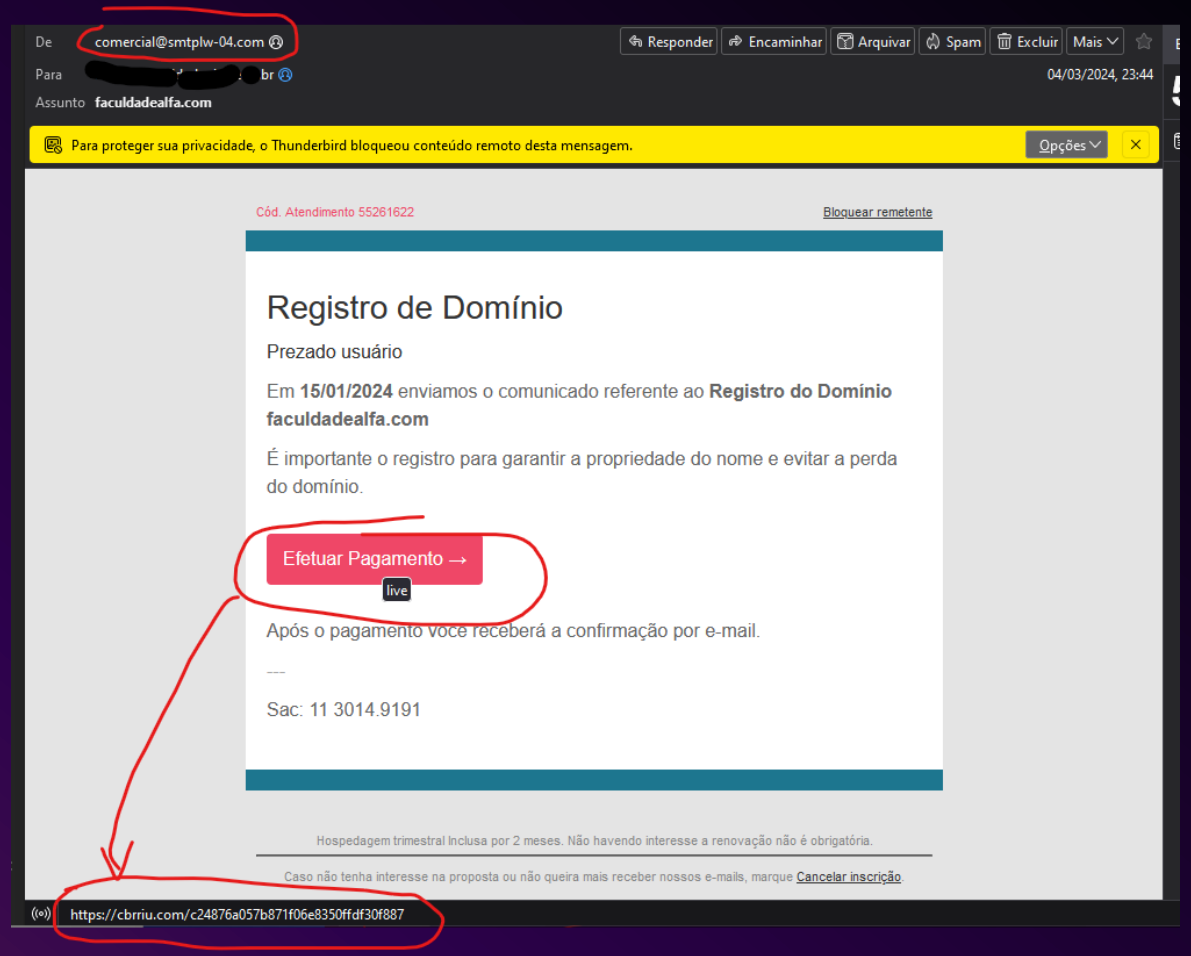
DENATRAN - Departamento Nacional de Trânsito

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.

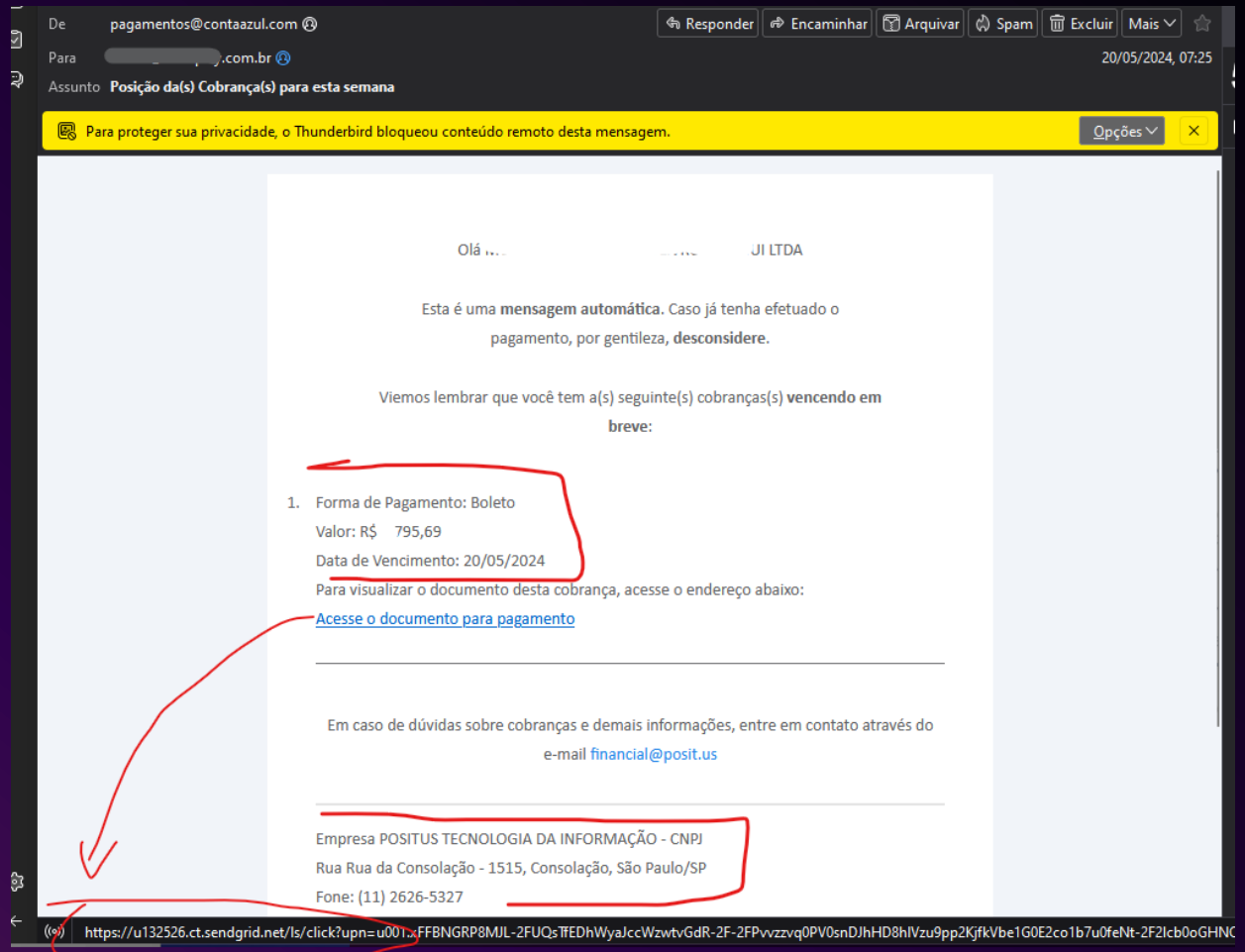
E-mail com domínios sem “.com.br” no final são suspeitos por serem internacionais e neste caso o e-mail veio como infracional-movel5360@b0mbeiros2024i.agencia-estatal.com tudo para tentar enganar, mas certamente é um golpe.

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

OBRIGADO

Daniel David Nunes

@daniel.davidnunes