

CRIMES

VIRTUAIS

PREVINA-SE



SEJUSP

SECRETARIA DE ESTADO DE JUSTIÇA
E SEGURANÇA PÚBLICA



GOVERNO DO
ACRE

Trabalho para cuidar das pessoas

SUMÁRIO

03 | Introdução

04 | O que é um crime virtual?

05 | Como prevenir crimes virtuais

- Senhas seguras
- Atualização de dispositivos
- Cuidados com links e arquivos
- Compartilhamento de dados pessoais
- Verificação em duas etapas

06 | Tipos de golpes

- Clonagem de WhatsApp
- Falsa identidade
- Falso call center
- Phishing / Links falsos
- Falso QR Code
- E-mail vazio

07 | Perfil fake

08 | Golpes comuns

- Golpe do Detran/IPVA
- Golpe do Pix
- Golpe do leilão / Boleto falso
- Golpe do Bolsa Família
- Golpe do emprego remoto
- Golpe do empréstimo falso

09 | Ameaças e crimes digitais

- Ameaça de morte / Falso sequestro / Assalto
- Golpe do amor / "Nudes"
- Golpe do bilhete premiado Inteligência artificial e clonagem de voz
- Uso indevido de plataformas digitais para cometimento de crimes

10 | Mais dicas de segurança

11 | Fui vítima de um crime virtual. O que fazer?

INTRODUÇÃO

A crescente utilização da internet e das tecnologias digitais traz inúmeras facilidades para o nosso cotidiano, no entanto tem gerado novos desafios, especialmente no que diz respeito à segurança online. No Estado do Acre, como em outras Unidades da Federação, os crimes virtuais têm se tornado uma preocupação crescente, afetando cidadãos, empresas e instituições públicas.

Para a **Secretaria de Estado de Justiça e Segurança Pública (SEJUSP)**, em um mundo cada vez mais conectado, a conscientização e o conhecimento sobre os riscos e as formas de prevenção são essenciais para proteger a população acreana. Esta cartilha tem como objetivo fornecer informações claras, objetivas e acessíveis sobre os principais tipos de crimes cibernéticos; como se prevenir de ataques virtuais e como agir em caso de ser vítima de algum golpe digital.

Por tanto, o presente material tem como objeto ser um guia prático e eficiente para que todos, desde estudantes até profissionais e instituições, possam entender e tomar medidas preventivas contra os riscos do mundo digital. A proteção da nossa vida online começa com a informação e o cuidado de cada um de nós.

O QUE É UM CRIME VIRTUAL

Crimes virtuais são crimes cometidos por meio da internet ou de dispositivos digitais, como computadores, smartphones e outros. Eles envolvem atividades criminosas, como fraude, roubo de dados e invasão de sistemas. A crescente utilização de tecnologia torna essas infrações cada vez mais comuns.



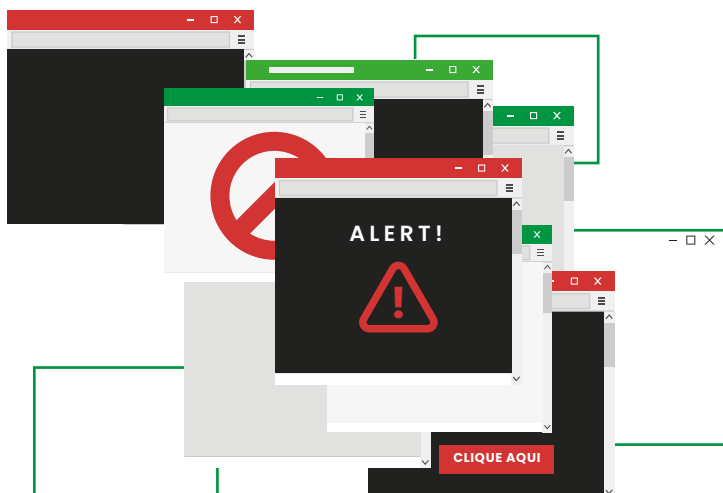
COMO PREVENIR CRIMES VIRTUAIS?

- Use senhas fortes e únicas para cada conta.
- Mantenha seu dispositivo atualizado com as últimas versões de sistemas operacionais e antivírus.
- Desconfie de links desconhecidos e nunca clique em links ou baixe arquivos de fontes suspeitas.
- Nunca compartilhe dados bancários ou pessoais por e-mail ou telefone.

VERIFICAÇÃO DE DUAS ETAPAS

A verificação de duas etapas é uma camada extra de segurança para proteger suas contas online.

- Ative a verificação de duas etapas sempre que possível. Isso adiciona um código enviado ao seu celular ou e-mail para confirmar sua identidade.



TIPOS DE GOLPES



WhatsApp/Clonagem

Os golpistas clonam seu número de WhatsApp e pedem dinheiro aos seus contatos.



Falsa Identidade

Criminosos se passam por outras pessoas para enganar suas vítimas.



Falso Call Center

São e-mails ou mensagens falsas que tentam obter seus dados pessoais.

DICA

Habilite a verificação em duas etapas no WhatsApp.

DICA

Confirme sempre a identidade de quem está te pedindo algo importante.

DICA

Não forneça informações sensíveis por telefone.



Phishing/Links

São e-mails ou mensagens falsas que tentam obter seus dados pessoais



Falso QR Code

Golpistas criam QR codes falsos para redirecionar para sites fraudulentos.



E-mail Vazio

E-mails sem conteúdo ou com anexos estranhos podem ser tentativas de golpe.

DICA

Desconfie de links estranhos e nunca clique sem verificar.

DICA

Verifique sempre o destino do link antes de escanear.

DICA

Apague e denuncie e-mails suspeitos.



Perfis falsos nas redes sociais são criados com o intuito de enganar as pessoas. Para evitar ser enganado:

- Verifique as fotos: faça uma busca reversa da imagem no Google;
- Desconfie de solicitações suspeitas;
- Evite compartilhar informações pessoais com estranhos.

GOLPES COMUNS



Golpe do Detran/IPVA

Golpistas se passam por órgãos públicos para solicitar pagamento de taxas falsas.

DICA Verifique sempre o site oficial do Detran ou da Secretaria da Fazenda.



Golpe do Pix/Falso

Fraudes envolvendo transferências via Pix.

DICA Confirme sempre os dados do destinatário antes de realizar transferências.



Golpe do Leilão/Falso Bolet

Anúncios falsos de leilões ou boletos fraudulentos.

DICA Verifique sempre o site oficial do Detran ou da Secretaria da Fazenda.



Golpe do Bolsa Família

Golpes que se aproveitam de benefícios sociais para enganar a vítima.

DICA Verifique sempre o site oficial do Detran ou da Secretaria da Fazenda.



Golpe do Emprego Remoto

Ofertas de empregos falsos que solicitam pagamento adiantado.

DICA Não pague nada para conseguir um emprego.



Golpe do Empréstimo Falso

Golpistas oferecem empréstimos com condições vantajosas.

DICA Desconfie de propostas que exigem pagamento antecipado.



Golpe do Bilhete Premi

Golpistas informam que você ganhou um prêmio, mas para recebê-lo você precisa pagar taxas.

DICA Não aceite ofertas de prêmios sem comprovação.



AMEAÇAS E CRIMES DIGITAIS

AMEAÇA DE MORTE/FALSO SEQUESTRO/ASSALTO

Golpes em que criminosos tentam extorquir dinheiro com falsas ameaças de violência.

DICA: Entre em contato com a polícia imediatamente, principalmente em casos de ameaças.

GOLPE DO AMOR/NUDES

Golpes emocionais em que golpistas se aproveitam de relações virtuais para extorquir dinheiro ou fotos íntimas.

DICA: Nunca compartilhe informações íntimas com desconhecidos na internet.

INTELIGÊNCIA ARTIFICIAL E CLONAGEM DE VOZ

Com o uso de inteligência artificial, é possível criar vozes e imagens falsas, o que pode ser utilizado para aplicar golpes.

Dica: Desconfie de mensagens de voz ou vídeo que pareçam estranhas ou fora do comum.

USO INDEVIDO DE PLATAFORMAS DIGITAIS PARA COMETIMENTO DE CRIMES

A internet e plataformas digitais, como redes sociais e aplicativos de mensagens, podem ser usadas para cometer crimes. É importante sempre denunciar abusos e ter cautela ao compartilhar informações online.



- Evite redes Wi-Fi públicas
- Quando possível, evite atender chamadas de números que não constam na sua agenda de contatos.
- Desconfie sempre de ofertas de produtos com preços abaixo dos praticados no mercado.
- Não converse com estranhos, tampouco aceite propostas que pareçam ser muito boas e que lhe trariam alguma espécie de “vantagem”.
- Exclua informações de natureza pessoal (RG, CPF, conta bancária, telefone, etc.) de seus aplicativos. Você não sabe se, eventualmente, perderá ou terá seu smartphone furtado.
- Desative Wi-Fi e Bluetooth quando não estiver utilizando.

BANCOS / FALSA CENTRAL ELETRÔNICA

- Bancos nunca ligam para cliente e pedem dados pessoais, senhas, atualizações de sistemas, chaves de segurança ou qualquer tipo de pagamento/transação para supostamente regularizar problemas na conta.
- Ao receber uma ligação suspeita solicitando senhas ou dados pessoais, desligue imediatamente e, de outro telefone, entre em contato com os canais oficiais de seu banco.



FUI VÍTIMA DE UM CRIME VIRTUAL! O QUE FAZER?

Se você for vítima de um crime virtual, siga estas orientações:

- Não entre em pânico;
- **Registre o incidente:** anote tudo o que aconteceu, incluindo hora, minuto e segundo. Guarde prints, e-mails, mensagens ou qualquer evidência;
- **Informe às autoridades:** a delegacia de crimes virtuais (ou a mais próxima de sua residência) é o local adequado para registrar a ocorrência. Outra alternativa é acessar o QR code da Delegacia Virtual do Ministério da Justiça e Segurança Pública para registrar boletim de ocorrência, caso seja vítima dos chamados "Golpes" cometidos pessoalmente, por telefone ou internet;
- **Altere senhas e bloqueie acessos:** proteja suas contas online;
- **Avise seus contatos:** caso a sua conta foi clonada, informe aos amigos e familiares sobre o golpe.



ACESSE

Delegacia Virtual do
Ministério da Justiça
e Segurança Pública

SEJUSP

SECRETARIA DE ESTADO DE JUSTIÇA
E SEGURANÇA PÚBLICA



GOVERNO DO
ACRE

Trabalho para cuidar das pessoas

PRODUÇÃO/REVISÃO

Ana Paula Xavier - Jornalista - DRT - 196

ASSESSORA DE COMUNICAÇÃO SOCIAL - SEJUSP

Daniele Carvalho de Souza

ASSESSORA DE IMAGEM E INFORMAÇÃO INSTITUCIONAL - SEJUSP

Paulo Sérgio Teixeira - Jornalista - DRT - 915

ANALISTA/REVISOR - SEJUSP

APROVAÇÃO

José Américo de Souza Gaia

SECRETÁRIO DE ESTADO DE JUSTIÇA E SEGURANÇA PÚBLICA

Evandro Bezerra da Silva

SECRETÁRIO ADJUNTO DE JUSTIÇA E SEGURANÇA PÚBLICA