PROTEÇÃO DO CELULAR

PNPC | PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

PNPC

Esta cartilha foi elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), desenvolvido pela Agência Brasileira de Inteligência (ABIN).

Criado em 1997, o PNPC é uma assessoria de segurança que busca promover cultura de proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas, com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

APRESENTAÇÃO

O celular é o principal meio de acesso à internet no Brasil, segundo a pesquisa TIC Domicílios de 2019, realizada pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (Cetic) do Comitê Gestor da Internet no Brasil (CGI.br). Os dados revelaram que 97% dos internautas brasileiros usam o smartphone para navegar. Você pode, inclusive, estar neste momento acessando esta cartilha pelo seu dispositivo móvel.

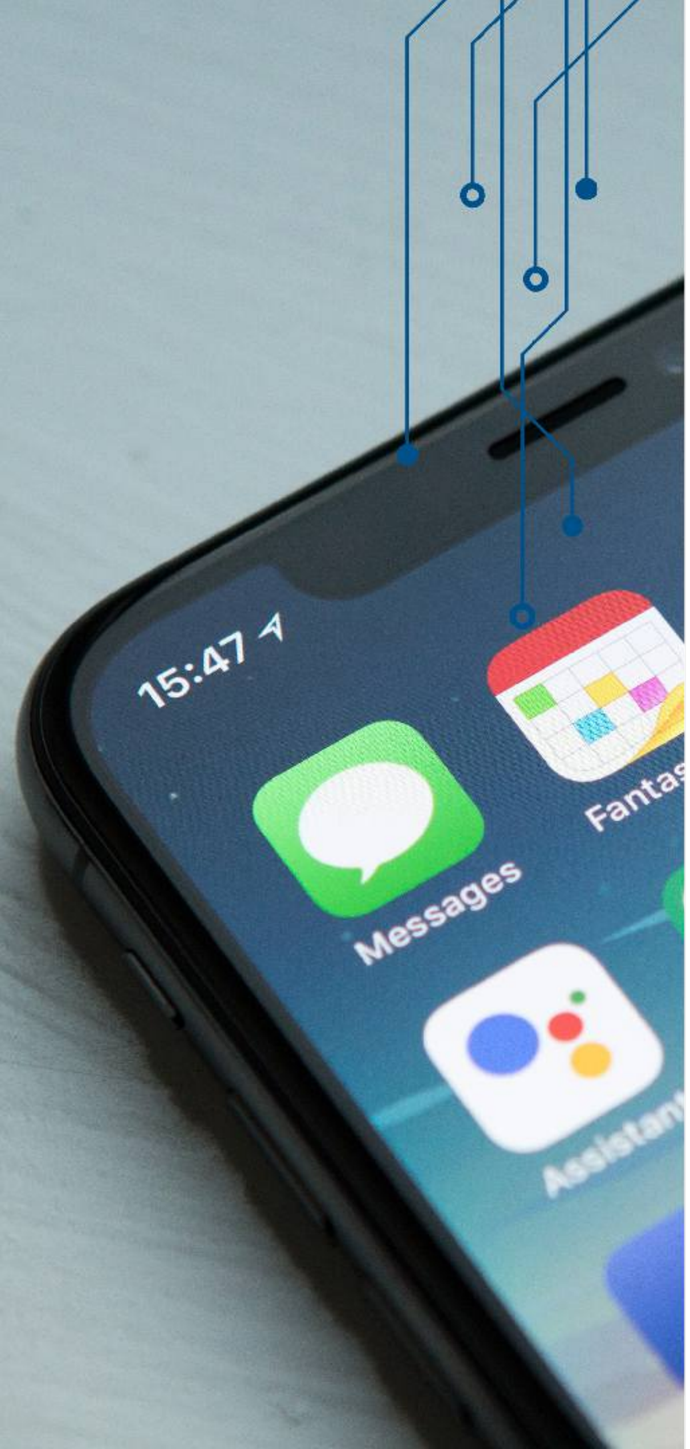
Da mesma maneira que universaliza o acesso à internet, o celular também facilita a ocorrência de crimes virtuais e ações de espionagem promovidas

por Estados, organizações estrangeiras e empresas concorrentes, por exemplo. Além disso, as ameaças estão sempre evoluindo e se adaptando aos nossos hábitos, por isso é importante você aprender a usar seu aparelho de maneira segura.

Nós, do PNPC, esperamos que esta cartilha seja um instrumento para que você se informe sobre como os ataques cibernéticos a dispositivos móveis acontecem, quais são os mais comuns no Brasil e também como se proteger desses ataques virtuais.

PNPC
PROTEGER COM INTELIGÊNCIA

1
APLICATIVOS DE CELULAR



Dentre os diversos aplicativos disponíveis para os usuários, existem aqueles desenvolvidos com a finalidade de execução de atividades maliciosas, ainda que pareçam confiáveis por oferecerem algum produto ou serviço.

Alguns programas maliciosos, como os chamados programas espiões *(spywares)*, conseguem ativar remotamente funcionalidades que o aparelho celular possui, tais como microfone, câmera, geolocalização e interceptação do que é digitado pelo usuário.

Além disso, determinados *spywares* são capazes de acessar dados do celular (contatos, mensagens, fotos, vídeos, arquivos do usuário etc.) e encaminhá-los secretamente a servidores na internet, controlados pelo atacante, com o propósito de receber esses arquivos.

Aplicativos espiões não são os únicos que coletam suas informações. Alguns aplicativos usados no dia-a-dia também podem ter essa finalidade, mesmo que de forma oculta. Ainda que alguns programas tenham motivos legítimos para guardar suas informações, eles também colocam sua privacidade em risco ao acessarem dados do seu celular. Essas informações podem ser repassadas para terceiros, como empresas que desenvolvem propaganda para alvos específicos a partir de um mapeamento de perfil de consumo.

Como se proteger?

- Instale um programa antimalware antes de baixar qualquer aplicativo.

- Baixe apenas aplicativos de lojas oficiais *(app stores)*.
- Leia as políticas de privacidade e pesquise sobre os aplicativos antes de baixá-los.
- Considere não baixar aplicativos com políticas vagas ou muito permissivas.
- Procure usar aplicativos de fontes confiáveis e que sejam bem avaliadas pelos usuários.
- Verifique se as permissões solicitadas pelo aplicativo estão de acordo com suas funções e propósitos.
- Evite instalar aplicativos usando contas de redes sociais (Facebook, Google) para evitar compartilhamento de

dados e formação de vínculos entre programas e bases de dados distintos.

- Instale versões mais recentes dos aplicativos, inclusive do antimalware, assim que estiverem disponíveis.
- Desinstale aplicativos que você não usa mais.
- Restrinja os acessos do aplicativo (localização, fotos, contatos etc.).
- Proteja informações pessoais (não forneça desnecessariamente dados como nome completo, endereço, telefone etc.).

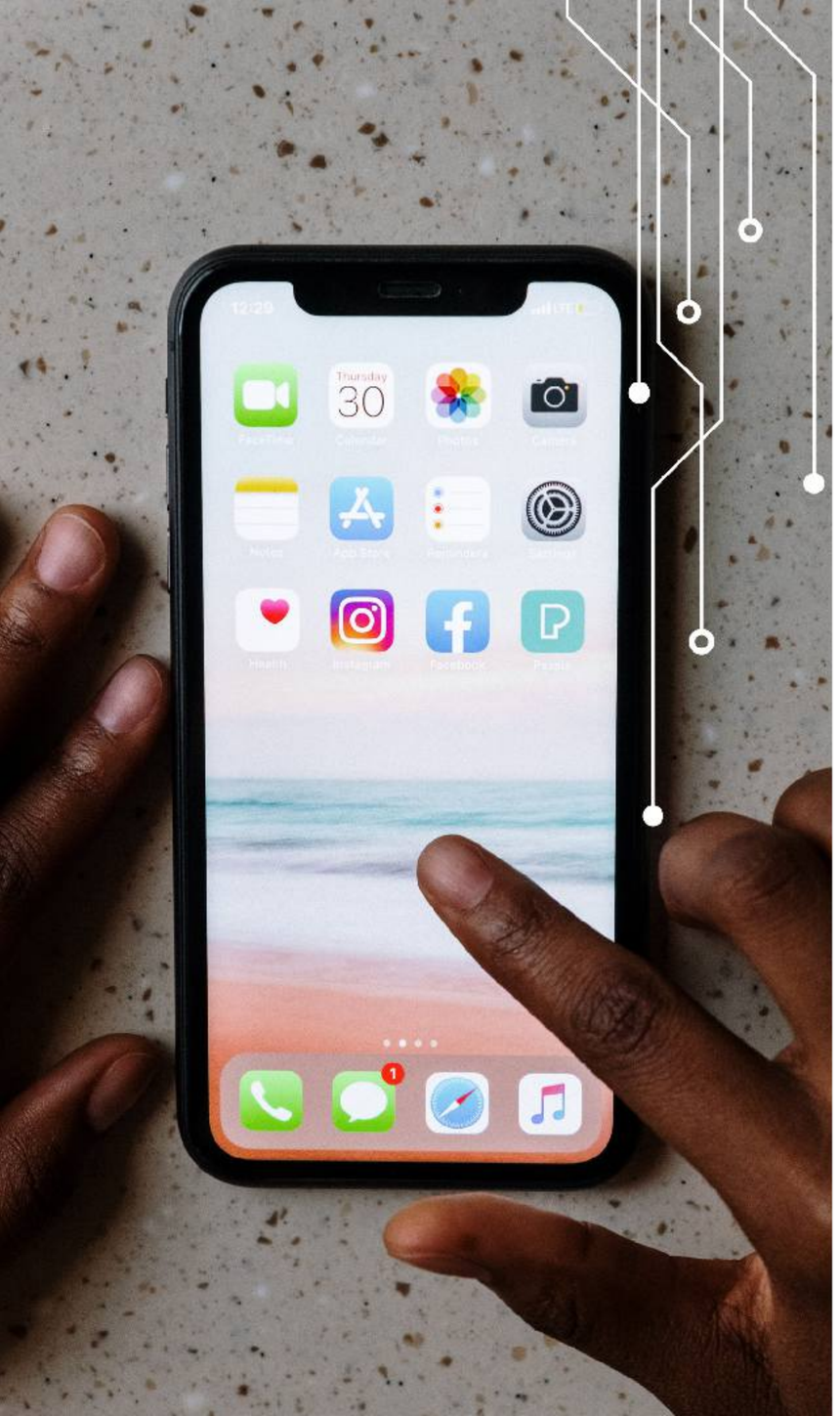
PNPC
PROTEGER COM INTELIGÊNCIA

2
APLICATIVOS DE MENSAGERIA

Aplicativos de mensageria são muito populares entre usuários de celular. Eles permitem o envio e o recebimento de diversos tipos de dados, desde mensagens de texto simples, até arquivos multimídia, PDF, planilhas, apresentações etc. Muitos aplicativos de mensageria são alvos potenciais de ações adversas em razão do tipo de informação que podem conter.

WhatsApp, Telegram e Signal

Alguns passos simples podem ampliar a sua segurança no uso do WhatsApp, Telegram, Signal e outros aplicativos de mensageria, para prevenir golpes e ações de espionagem:



- Ative a confirmação em duas etapas (também conhecido como segundo fator de autenticação – 2FA). A função verificação em duas etapas serve como mecanismo adicional de proteção após períodos de tempo, seja pelo aparelho ter sido desligado ou por não haver sido conectado por certo período. Essencialmente, é uma medida adicional de segurança em caso de perda ou furto/roubo do aparelho celular.

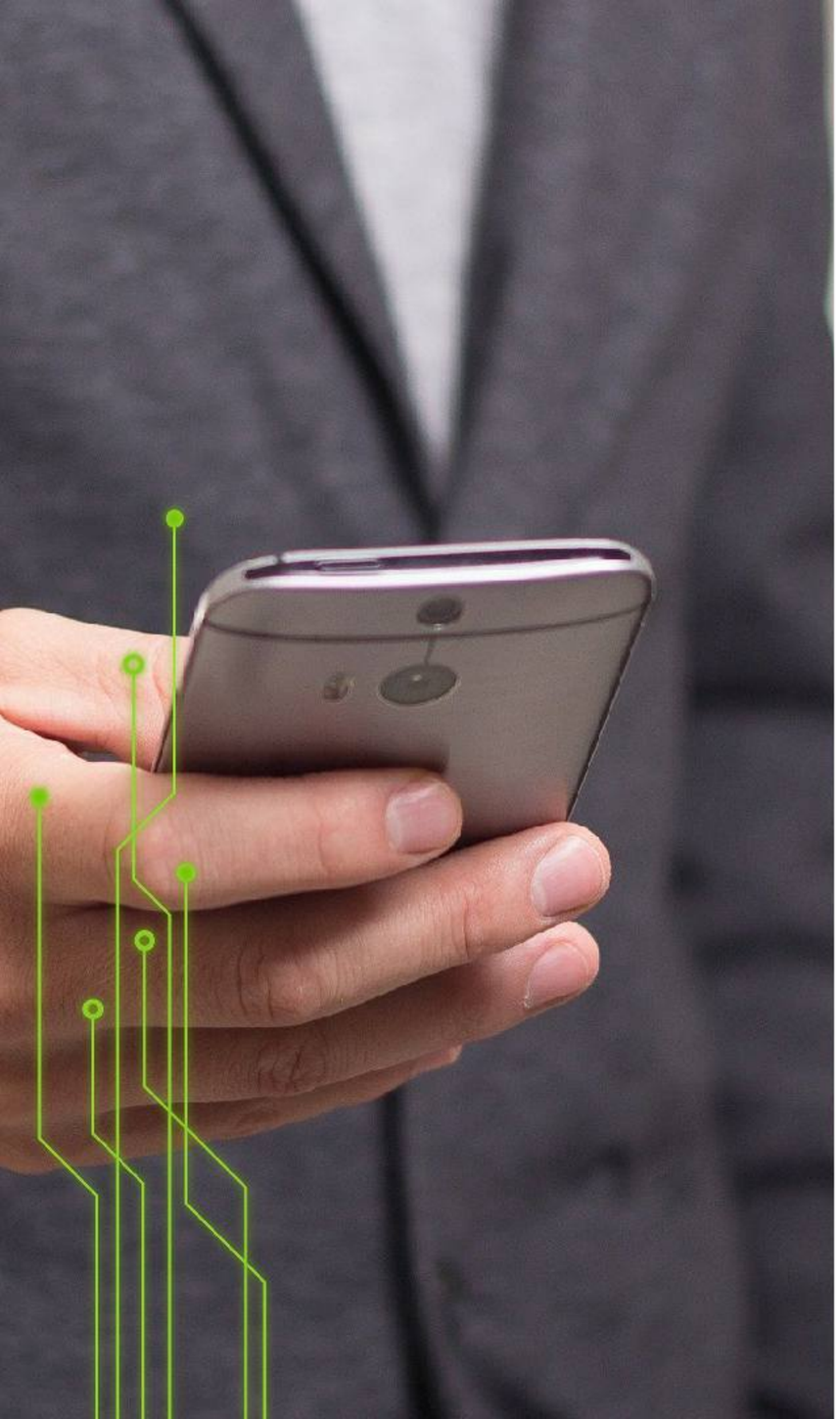
- No caso do WhatsApp, acesse “Configurações > Conta > Confirmação em duas etapas > Ativar” e siga o procedimento que será apontado na tela. Periodicamente, o WhatsApp vai pedir essa senha para dar acesso ao aplicativo como uma espécie de lembrete;

- Para ativar a funcionalidade no Telegram, acesse “Configurações > Privacidade e Segurança > Verificação em Duas Etapas” e siga o procedimento, configurando a senha, uma dica para se lembrar dela e um e-mail de recuperação;

- No aplicativo Signal, acesse “Configurações > Privacidade > Lembretes de PIN” e habilite a função. Também habilite a função “Bloqueio de Registro”.

PNPC
PROTEGER COM INTELIGÊNCIA

3
APARELHO CELULAR



Os celulares também ficam expostos a atividades maliciosas quando não estão protegidos fisicamente pelo proprietário ou quando ferramentas como wi-fi, bluetooth e localização estão ativadas desnecessariamente. Além disso, todo celular possui um sistema operacional com funcionalidades de segurança que podem ser habilitadas pelo usuário para proteção dos dados no aparelho.

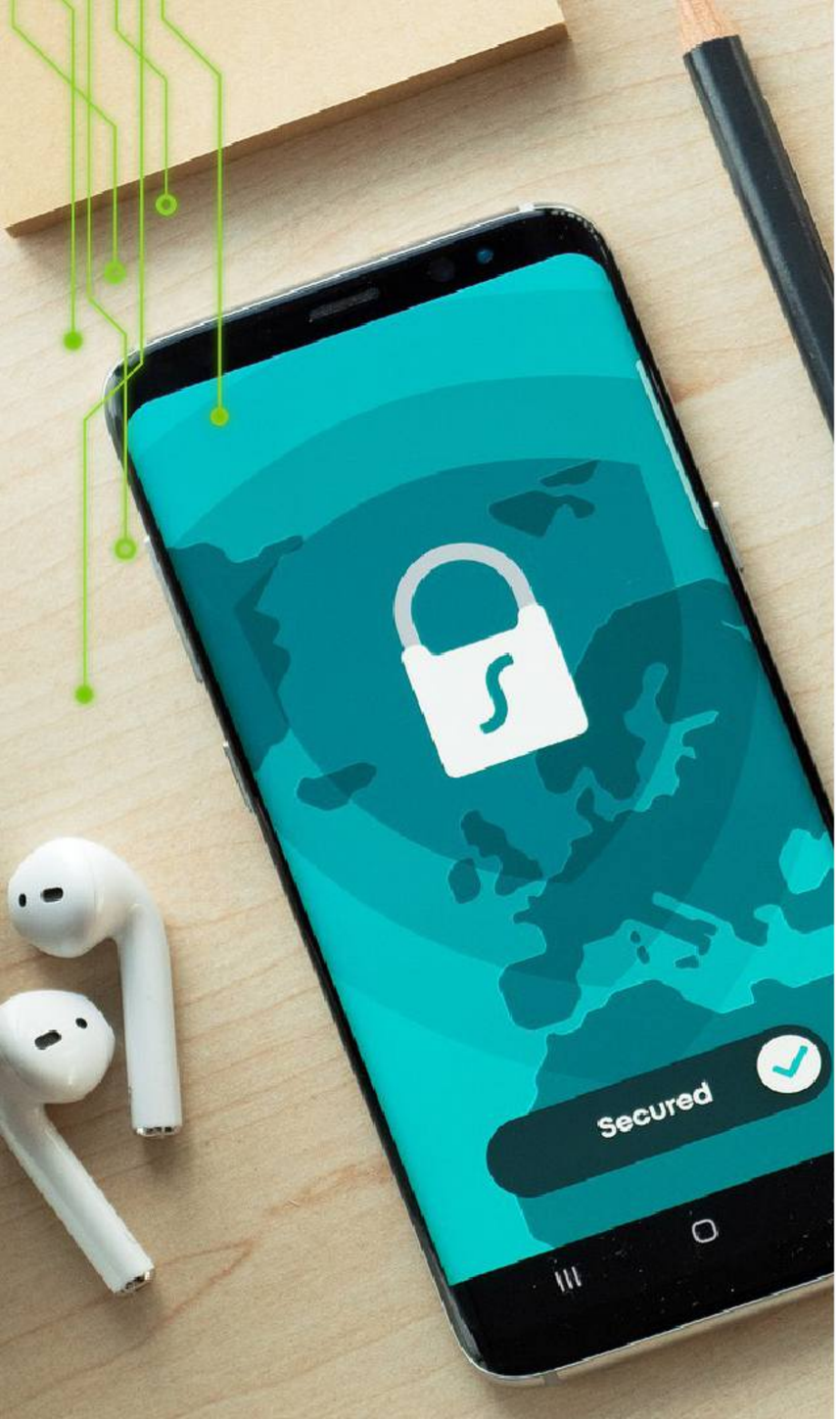
Como proteger o celular?

- Use conexões seguras e de fontes confiáveis.
- Evite wi-fi de ambientes públicos, inclusive aeroportos.

- Evite carregar seu celular em computadores e carregadores públicos via cabos USB.
- Desligue wi-fi, bluetooth e localização quando não estiverem em uso.
- Configure a conexão bluetooth para que seu dispositivo não seja identificado por outros dispositivos (modo “oculto” ou “invisível”).
- Desative notificações na tela.
- Habilite o bloqueio automático de tela.
- Mantenha o sistema operacional do celular atualizado com a última versão recomendada

pelo fabricante.

- Evite compartilhar o celular com pessoas que não precisam saber o que você possui instalado nele.
- Habilite mecanismos de segurança, tais como criptografia da memória de armazenamento e fator duplo de autenticação.
- Não conecte cartões de memória externa de fontes não confiáveis.
- Não compartilhe sua senha com outras pessoas e nem repita senhas.
- Não abra links de SMS (mensagem).

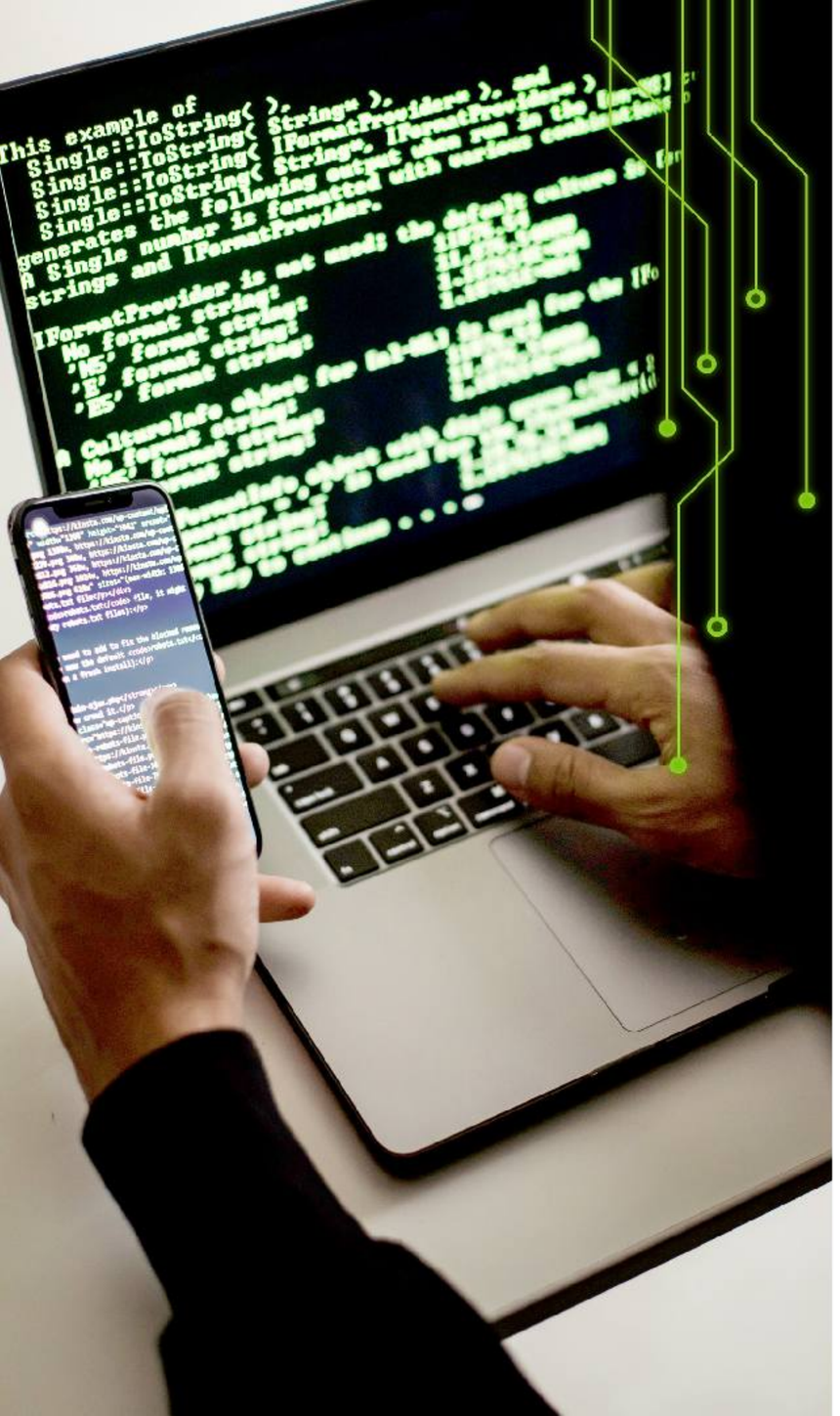


- Em caso de perda ou furto, solicite à operadora o bloqueio do seu número (chip) e altere as senhas armazenadas no celular (e-mail, redes sociais etc.).

- Ao se desfazer do seu smartphone, apague todos os dados e restaure as opções de fábrica.

PNPC
PROTEGER COM INTELIGÊNCIA

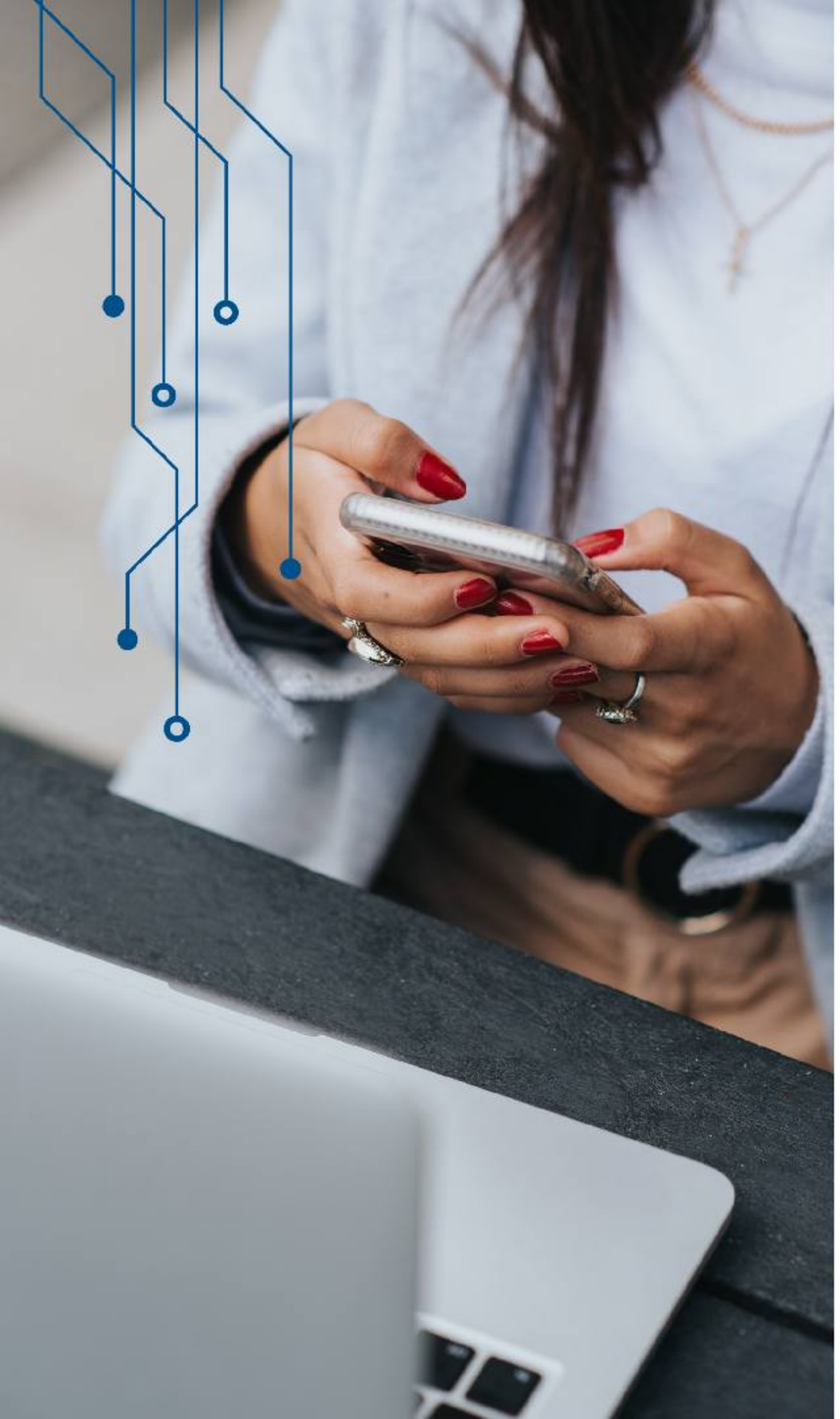
4
ATAQUES CIBERNÉTICOS



Cada vez mais, grupos criminosos têm se especializado em explorar as vulnerabilidades de equipamentos móveis, de sistemas operacionais ou do uso inseguro de dispositivos pelos usuários. Seguem alguns exemplos de tipos de ataque.

Spoofing

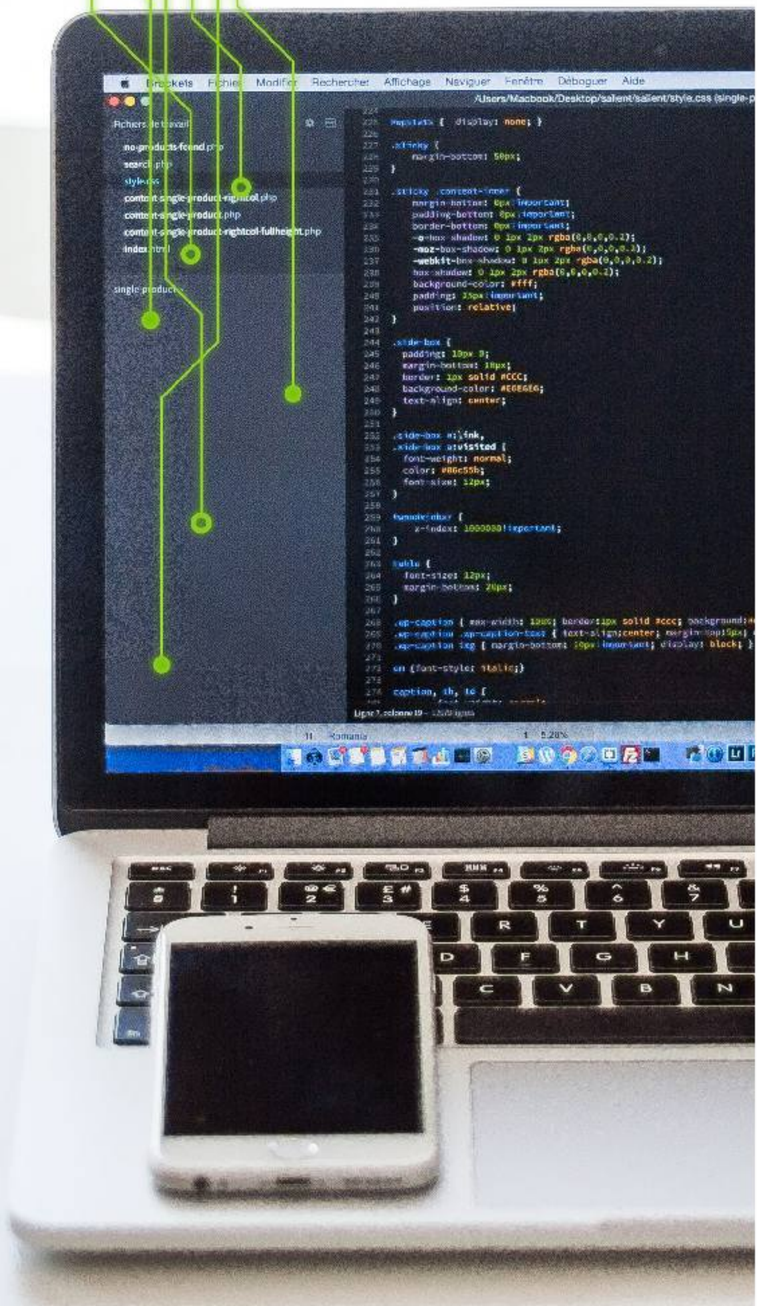
Spoofing é um termo que vem da palavra em inglês *“spoof”*, que significa “enganar” e consiste em uma técnica usada por hackers para falsificar a identidade de alguém em meios digitais e distribuir vírus ou interceptar informações legítimas, como dados bancários e mensagens pessoais.



O recurso é muito utilizado no Brasil, frequentemente em golpes em serviços de mensageria, nos quais o criminoso se apodera da conta de alguém para enviar mensagens pedindo dinheiro para os contatos do usuário prejudicado.

Os tipos de *spoofing* mais relacionados com crimes virtuais que ocorrem em celulares são:

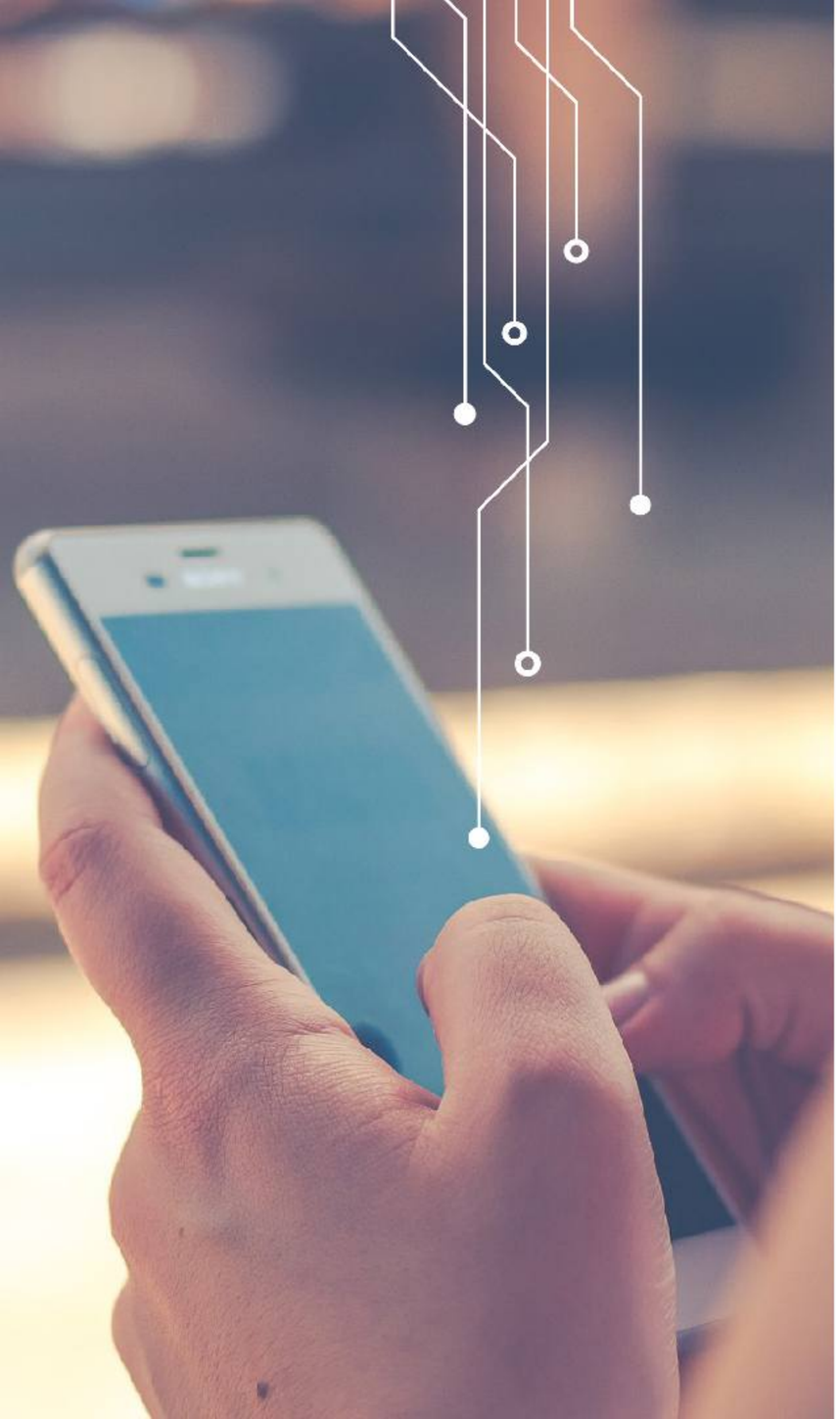
- *Spoofing* de Identificador de Chamadas (Caller ID): essa modalidade de ataque envolve a imitação de uma linha telefônica. Nesses casos, um hacker pode fazer ligações usando um chip qualquer e fazer com que o número da vítima apareça no identificador de chamadas no smartphone do destinatário.



- *Spoofing* de SMS: esse tipo de falsificação envolve a ocultação da linha telefônica que remete a mensagem. Nesse caso, um hacker pode usar essa modalidade de *spoofing* para se passar por instituição bancária e pedir informações sigilosas por mensagem.

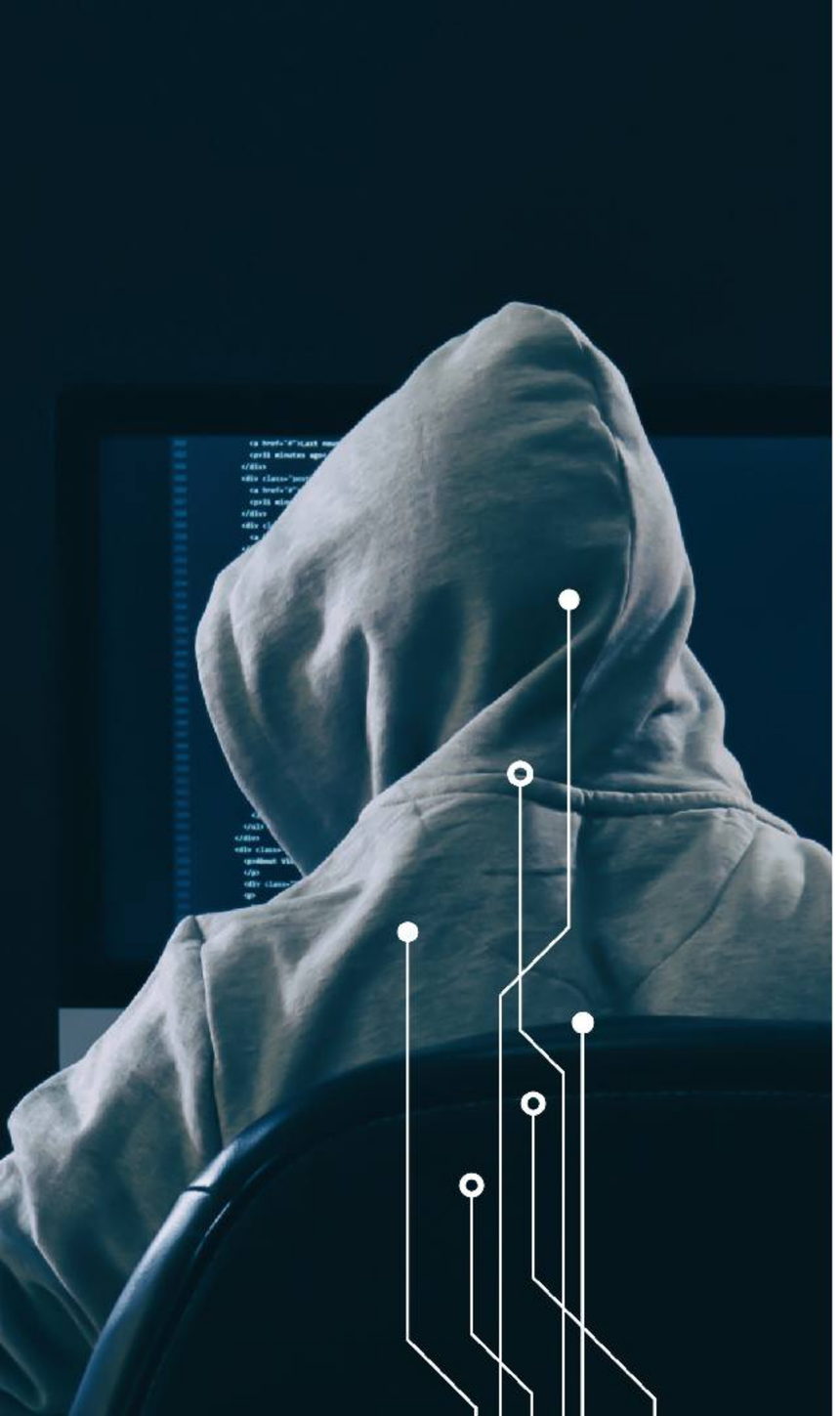
Phishing

Você já recebeu mensagens SMS de números completamente estranhos prometendo um prêmio ou solicitando o cadastramento de nova senha bancária? Neste caso, você provavelmente sofreu uma tentativa de ataque muito comum em dispositivo móvel chamada *phishing*. Este ataque tem como característica enganar o usuário,



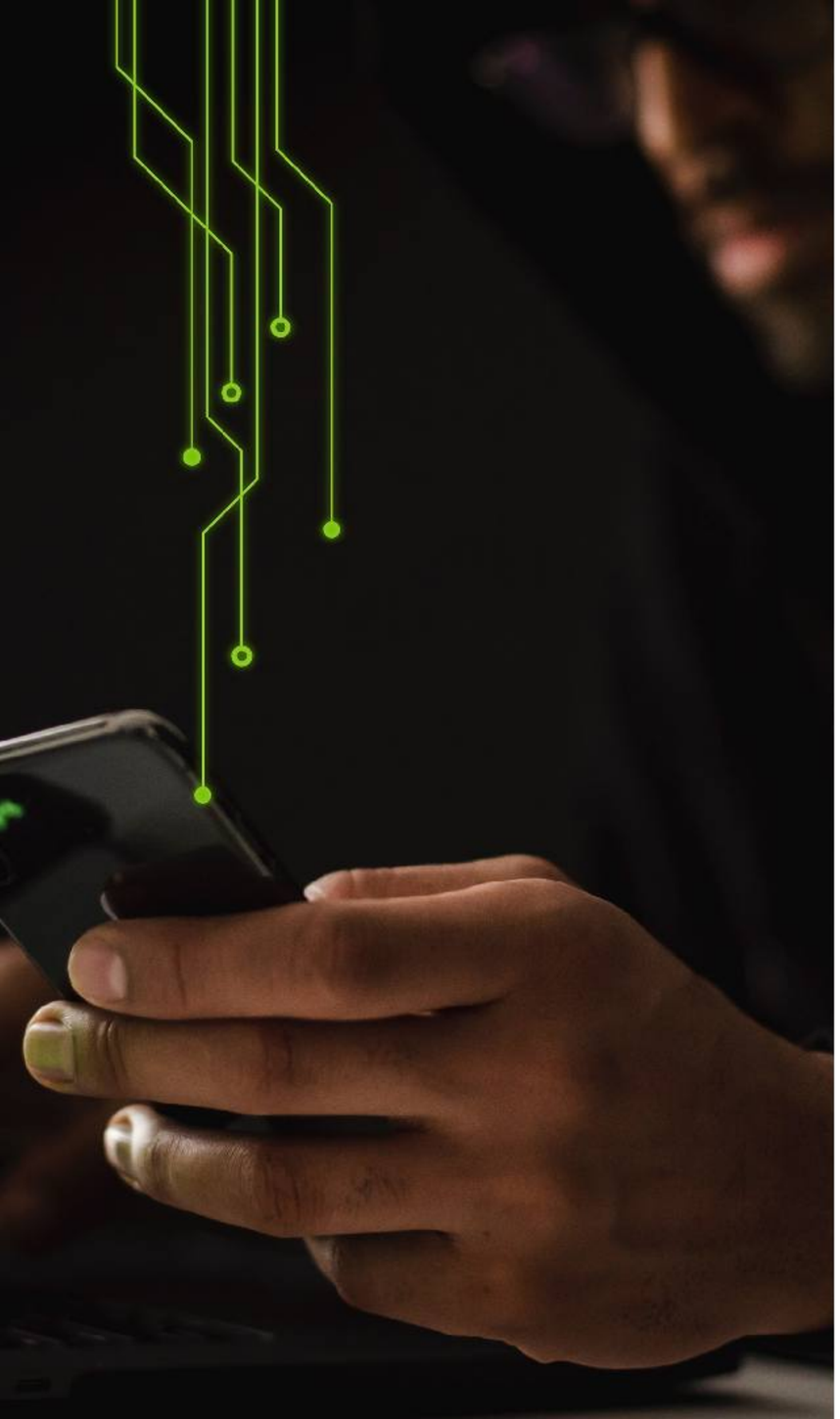
direcionando-o a sites maliciosos para roubar informações importantes. Geralmente o *phishing* está relacionado a:

- Promoções
- Mensagens que pedem seus dados
- Mensagens de prêmios
- Mensagens pedindo atualização de dados cadastrais
- Mensagens, inclusive de amigos vítimas de golpes, com links de aplicativo para download



Ataque de força bruta

Você sabia que pode ser alvo de uma infinidade de ataques, bem sucedidos ou não, mesmo sem perceber? O objetivo do ataque chamado de força bruta, ou *brute force*, é adivinhar um usuário e senha por meio de diversas tentativas. Isso pode ser feito de forma manual, com acesso físico ao seu celular, ou por meio de ferramentas automatizadas que reduzem o tempo para descobrir a senha. Entre as ações que o atacante pode efetuar em seu dispositivo estão:



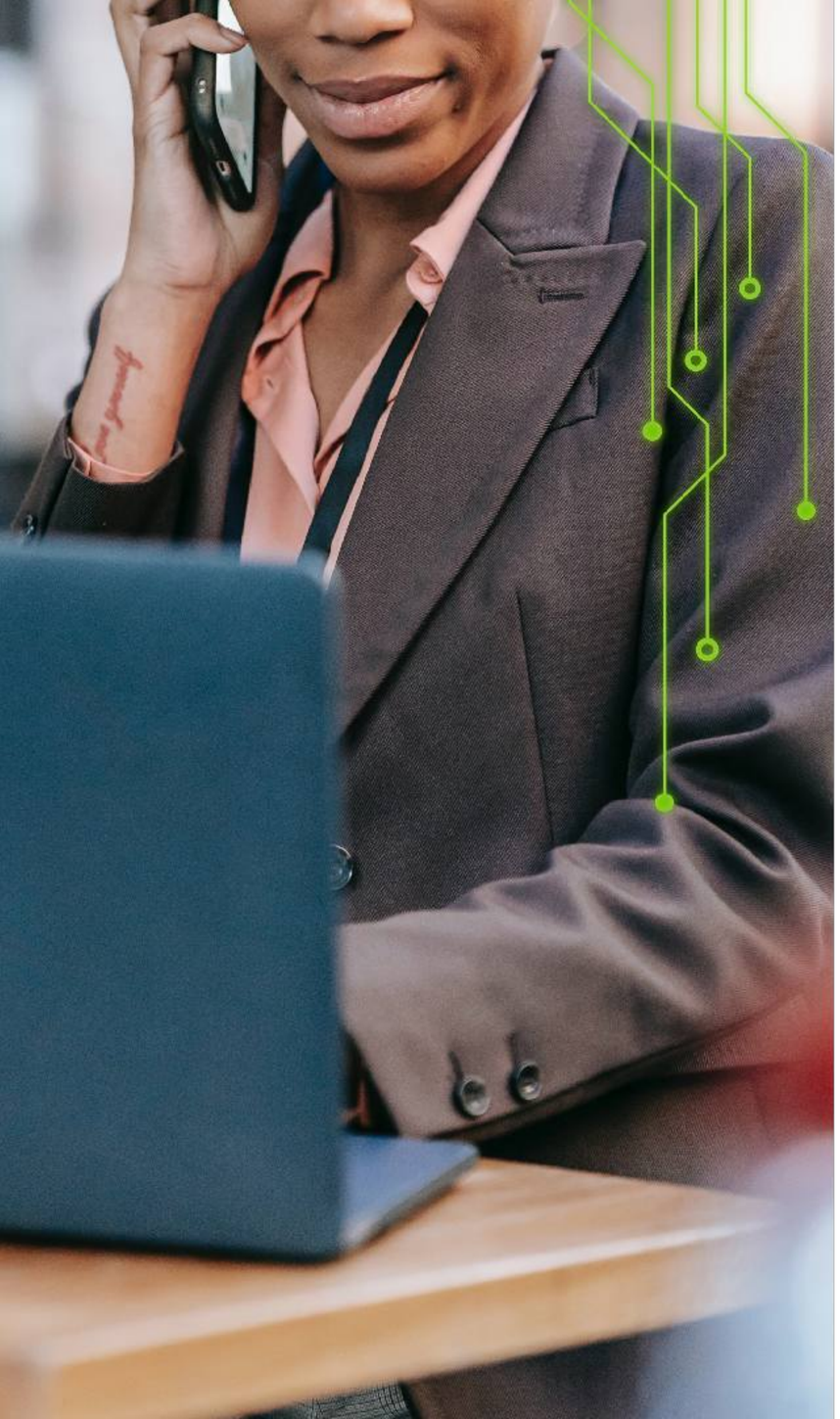
- Enviar mensagens falsas aos contatos de WhatsApp.
- Enviar links aos seus seguidores de redes sociais com códigos maliciosos.
- Obter informações confidenciais.
- Acessar aplicativos de bancos.
- Trocar sua senha.

PNPC

PROTEGER COM INTELIGÊNCIA

5

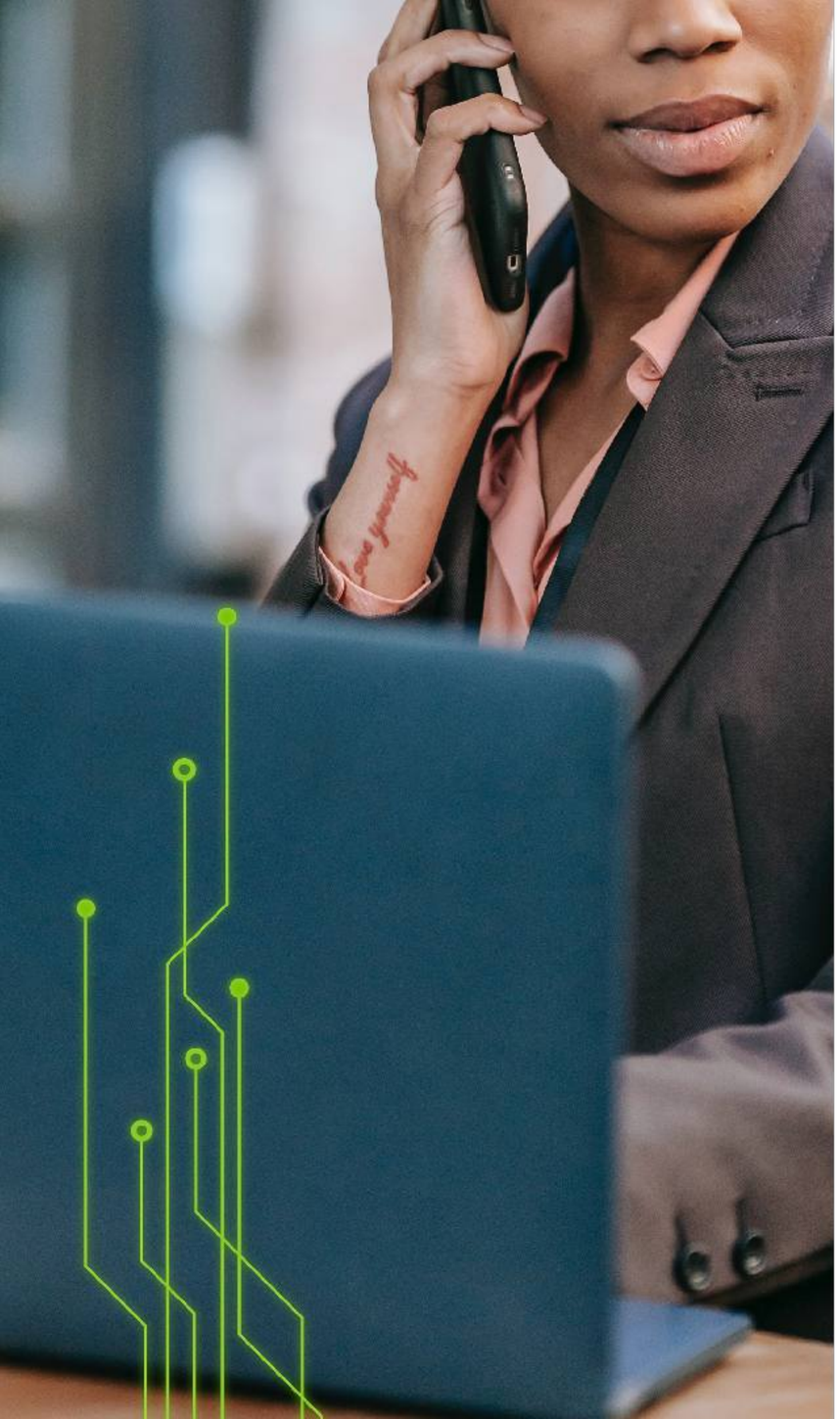
TELEFONEMAS



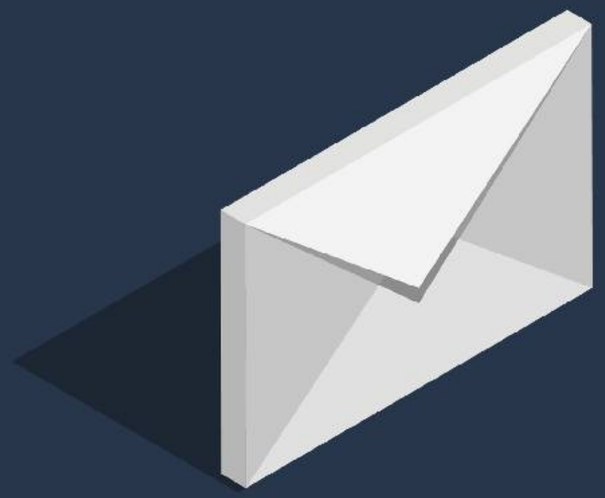
Chamadas telefônicas também podem ser usadas para coletar suas informações.

De que desconfiar?

- Ligação suspeita em que desconhecido tenta levantar nomes de pessoas com acesso a informações da instituição/empresa
- Perguntas muito detalhadas e específicas
- Questões sobre acessos, responsabilidades, atividades etc. para identificar possíveis alvos
- Questões sobre a vida pessoal, para depois utilizar em outras ações



- Pedidos de e-mails e telefones pessoais
- Utilização de nome conhecido em comum, sem que a pessoa de fato o conheça
- Insistência mesmo quando informações são negadas
- Mesmo tipo de ligação para mais de uma pessoa do setor da instituição/empresa.



Reporte

Caso acredite que sua instituição foi vítima de ação de espionagem ou sabotagem, avise sua chefia e o setor de segurança. Você também pode enviar e-mail a **reporte@abin.gov.br** para estabelecer contato com a ABIN e relatar o caso.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR

WWW.GOV.BR/ABIN/PNPC