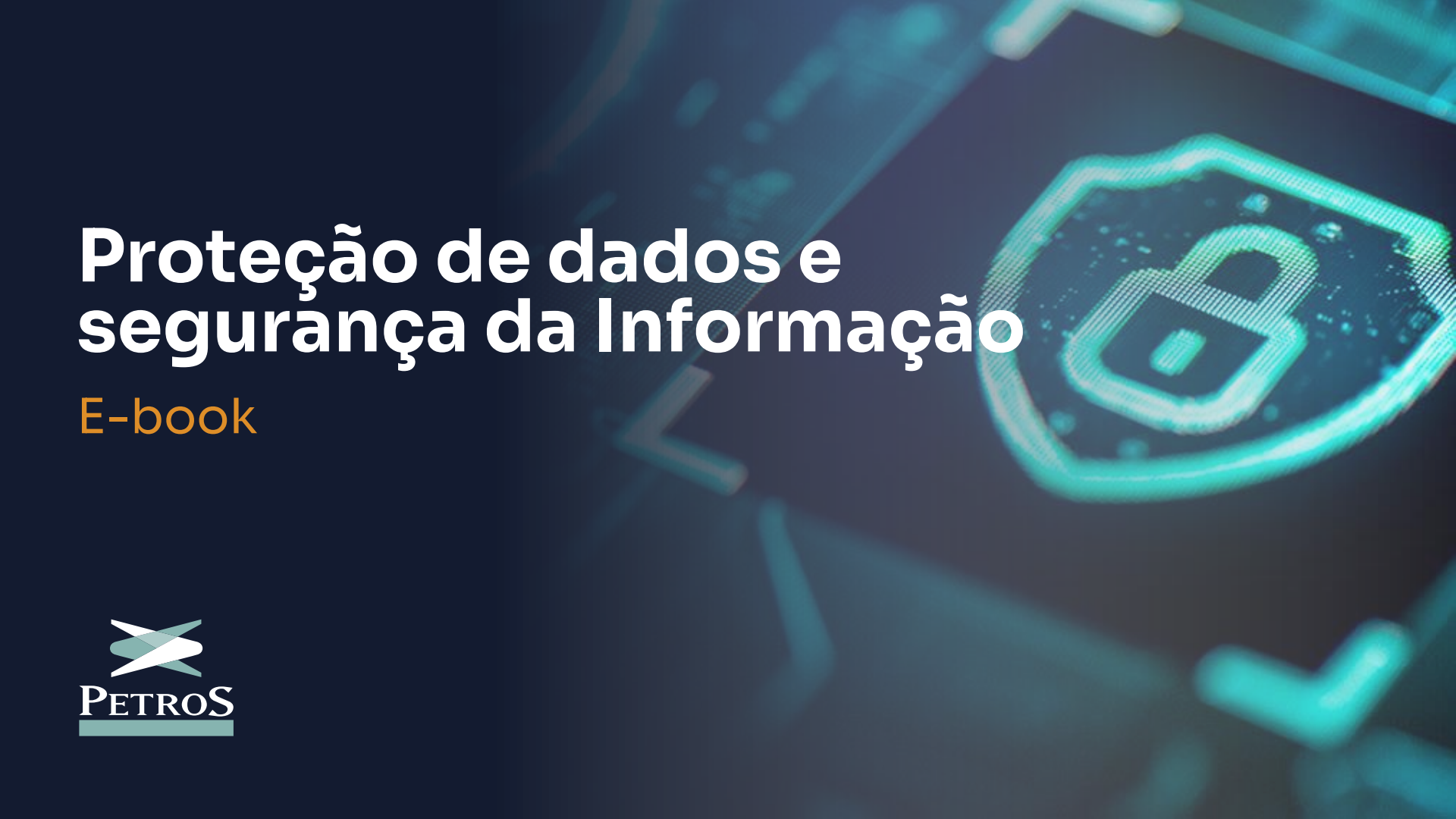
Proteção de dados e segurança da Informação

E-book



PETROS

Sumário

Clique no capítulo para acessar o conteúdo

Apresentação 3
Como normalmente funcionam os golpes? 4
Autenticação e senhas 5
Principais cuidados na internet 8
O que fazer ao clicar em um link suspeito 15
Golpes comuns 16
O que a Petros faz pela segurança dos meus dados 22
Nossos canais oficiais 23

Apresentação

A **Segurança da Informação** é um tema fundamental na Petros, sendo tratado com muita responsabilidade. Trabalhamos para proteger nossas estruturas e processos digitais, bem como nossas informações e os dados dos nossos **participantes**.

Sabendo da importância deste tema, preparamos um **e-book** com dicas que podem ser adotadas para **utilizar a internet com mais segurança.**

Nele, apresentamos cuidados essenciais para a **proteção de senhas** e **dados pessoais**, além de mostrar como se prevenir contra armadilhas virtuais.

Confira a seguir e **boa leitura**!

Como normalmente funcionam os golpes?

Os golpes podem ser aplicados de diversas formas e por diferentes meios, como **e-mails**, **SMS**, **ligações telefônicas**, **cartas** e até **presencialmente**.

Pessoas mal-intencionadas **induzem a vítima** a **fornecer dados pessoais** ou realizar ações que causem prejuízos, principalmente financeiros.

Buscando solucionar rapidamente um problema, muitas pessoas acabam fornecendo suas **senhas**, **dados pessoais** e **códigos de acesso** para golpistas que se passam por empregados de empresas ou instituições financeiras.

Somente depois, a vítima percebe que **caiu em um golpe**.

Autenticação e senhas seguras

Melhores práticas

- Utilize **números aleatórios**.

- **Use grande quantidade de caracteres, quando possível:** quanto mais longa e complexa for a senha, mais difícil será descobri-la (recomenda-se, no mínimo, 8 caracteres contendo letras maiúsculas, minúsculas, caracteres especiais e números).

- **Utilize diferentes tipos de caracteres, quando possível**: busque misturar ao máximo caracteres como números, sinais de pontuação e letras, variando entre maiúsculas e minúsculas.

- **Troque sua senha periodicamente**: nunca utilize a mesma senha para acessar mais de uma conta ou aplicativo.

O que não fazer

- **Não use qualquer tipo de dado pessoal:** evite usar seu nome e sobrenome, números de documentos, placas de carros, números de telefones e datas de aniversário, por exemplo.

- **Não utilize sequências de teclado:** evite senhas associadas a botões que sejam próximos, como “QwerT” e “1qaz”. Não utilize trechos do alfabeto ou ordem numérica, como “abc1234”.

- **Evite termos e nomes publicamente conhecidos:** como nomes de empresas, nomes de times de futebol, títulos de músicas etc.

- **Não utilize uma mesma senha** para múltiplos serviços.

IMPORTANTE

- Muitos **sites**, **aplicativos**, **e-mails** e **perfis em redes sociais** oferecem a **verificação em duas etapas**. Ative essa opção **sempre que possível**.
- Evite deixar seus **dados** e **senha** salvos para **acessos automáticos** na próxima vez que você for usar o serviço.
- **Nunca anote senhas** e dados **pessoais** no bloco de notas do seu notebook e celular.

Principais cuidados na Internet

Clique nos temas abaixo e confira algumas **dicas de cuidados básicos** para navegar na Internet com mais segurança:

- **Wi-Fi Público**
- **Aplicativos para dispositivos móveis**
- **Phishing**

Wi-Fi Público

- **Verifique as informações da rede:**

  Confirme se o nome da rede Wi-Fi está relacionado ao local ou estabelecimento em que você está. Não se conecte em redes que você não sabe de onde veio.

- **Preserve sempre seus dados:**

  Não digite senhas e outras informações pessoais quando estiver conectado nestes tipos de redes.

- **Não compartilhe arquivos:**

  O envio ou o download de arquivos usando redes públicas pode trazer riscos de comprometimento para o seu dispositivo. Fique atento!

- **Desconecte-se ao finalizar o uso:**

  Não deixe o acesso ativo quando terminar de utilizar a internet. Neste tipo de rede, você está conectado a outras pessoas. Por isso, neste meio tempo, cibercriminosos podem invadir o seu dispositivo.

Aplicativos para dispositivos móveis

- Nunca instale apps que não estejam nas lojas oficiais do Android e do iOS.
- Não instale apps de empresas e fontes desconhecidas.
- Mantenha os aplicativos de seus dispositivos sempre atualizados.

Tenha acesso aos nossos serviços na palma da sua mão!

Aponte a câmera do seu celular para os **QR Codes** e faça o download do **App Petros** diretamente pelas lojas oficiais da **iOS** e **Android**:

DISPONÍVEL NA App Store

DISPONÍVEL NO Google Play

Phishing

O que é?

Phishing é o ato ilícito de “pescar” usuários para roubar suas informações como CPF, nomes, senhas e, com isso, praticar crimes cibernéticos.

E, para pescar, é preciso de uma isca. No caso do phishing, a isca costuma ser um link enviado por e-mail, mensagens de texto ou aplicativos de mensagens. Por isso, é preciso ficar bastante atento para não clicar em links ou acessar sites suspeitos. Esses links podem redirecionar você para uma situação de golpe.

Atenção:

Caso perceba uma tentativa de phishing ou outro golpe usando o nome da Petros, denuncie pelo **Fale Conosco** ou pelo chat on-line, disponíveis no **Portal Petros** e no nosso **aplicativo**. Ou ligue para a **Central de Relacionamento**, pelo número **0800 025 35 45**.

Como se prevenir contra esse golpe

• Ao receber e-mails, fique sempre atento ao **endereço eletrônico** do remetente. E quando for clicar em links de sites, verifique o domínio do endereço que vem **após o www**.

• **Não passe sua senha** para outras pessoas e nem realize **operações financeiras** solicitadas por contato telefônico ou mensagem de texto. **Desconfie sempre!**

• Desconfie de mensagens com **erros de ortografia** ou **gramática**.

• Suspeite sempre de **mensagens urgentes** que abordem temas relacionados a perdas financeiras, principalmente. Esta é uma estratégia bastante comum utilizada por golpistas.

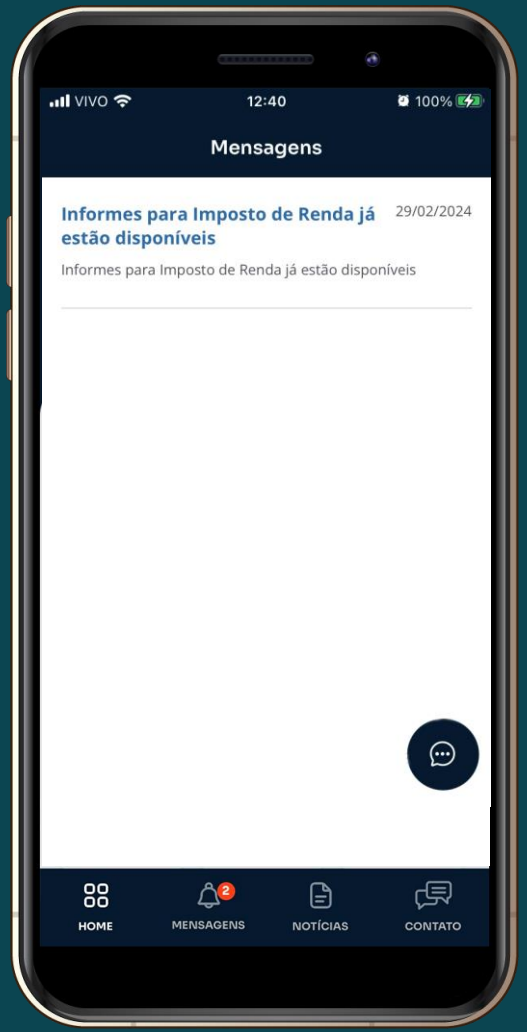
• Desconfie de e-mails de promoções ou descontos imperdíveis com link direto para concluir operações por PIX ou boletos, por exemplo. **Não clique em nada, até ter certeza de que o e-mail é real**. Se necessário, entre em contato com a instituição que enviou a mensagem e confirme a autenticidade do que foi solicitado.

IMPORTANTE

A Petros só envia links **por e-mail** e **mensagens de SMS** para o **e-mail e telefone de contato cadastrados** pelo participante junto à Fundação, seguindo as regras mencionadas anteriormente.

Por **aplicativo**, os textos são encaminhados pela aba "**mensagem**" dentro do **app** ou via **notificação *push****, caso o usuário autorize.

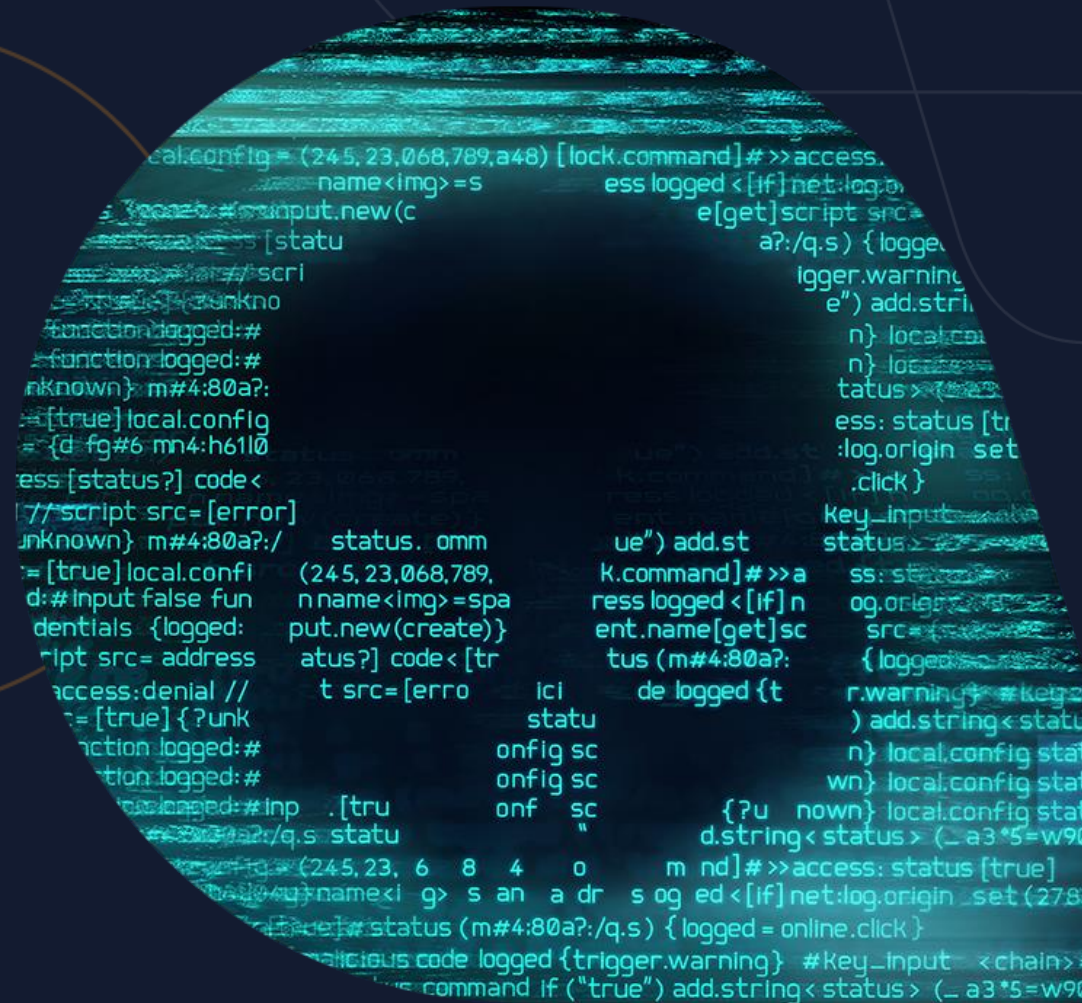
* Notificação *push*: são alertas de textos, banners ou pop-up que aparecem na tela do celular, diretamente na barra de notificações, sem a necessidade do aplicativo estar aberto no seu dispositivo.



O QUE FAZER AO CLICAR EM UM LINK SUSPEITO

- Feche **imediatamente** o site, **exclua arquivos** e **e-mails recebidos**.
- **Desinstale apps** que tenha baixado a partir da **mensagem suspeita**.
- Utilize um **antivírus** para fazer uma **varredura de segurança** em todos os seus dispositivos digitais (celular, computador, tablet etc.).

Golpes comuns



Golpe da oferta de serviços financeiros

Ofertas de serviços como **empréstimo consignado**, promessas de **liberações de crédito** ou **antecipações de dinheiro** mediante depósito antecipado, principalmente para pessoas negativadas, **podem ser golpes**!

Os golpistas se identificam como profissionais de uma empresa específica e solicitam os **dados pessoais**, **bancários** e **fotos**. Com as informações em mãos, os cibercriminosos conseguem realizar operações financeiras, **sem a permissão da vítima**.

Fique atento!

Os golpistas podem ainda solicitar **depósitos de valores** para que os golpes sejam encerrados. Contudo, não há **nenhuma garantia** de que os dados não serão novamente utilizados para outras ações deste tipo.

Golpe do Imposto de Renda

O golpe costuma ser aplicado utilizando os seguintes métodos:

Ligações fraudulentas: falsos agentes fazem ligações solicitando dados pessoais ou pagamento sob a alegação de erros na declaração. Eles ameaçam com penalidades, caso exigências não sejam cumpridas.

Aplicativos e sites falsos: criminosos criam aplicativos e sites falsos que imitam portais e apps governamentais oficiais para capturar informações pessoais e financeiras ou infectar seu dispositivo com arquivos maliciosos.

Falsos contadores: golpistas se passam por contadores e oferecem serviços a preços baixos. Após obterem os dados e o pagamento pelo serviço, eles desaparecem, podendo usar suas informações para cometer crimes.

Dica para evitar esse golpe:

- Mantenha-se informado por meio de canais de comunicação confiáveis;
- Não forneça dados pessoais (a Receita Federal não solicita informações por telefone ou e-mail); e
- Em caso de suspeita de fraude, informe à Receita Federal.

Golpe das centrais de atendimento

Para obter dados sensíveis, como número de contas, CPF, senhas etc., golpistas conseguem **mascarar o número real do telefone** que está originando a ligação, simulando que o contato está sendo feito de uma central de atendimento de uma instituição verdadeira. Fique atento e **prefira sempre entrar em contato diretamente com a empresa** e **confirmar se a solicitação é real**.

Outra forma bastante comum do golpe acontece a partir do envio de mensagens por SMS. Mensagens de textos informam sobre **falsas transações financeiras que estão em análise**, destacando que para cancelá-las é necessário ligar para um número específico, que não corresponde ao telefone oficial da empresa mencionada.

Atenção:

Os contatos por SMS da Petros **nunca acontecem por números convencionais**. E não enviamos mensagens por WhatsApp ou por outros aplicativos de mensagens, como o Telegram.

Golpe dos sites falsos

Cibercriminosos criam **sites idênticos** ou **muito parecidos** com os reais, buscando enganar as vítimas. Isso normalmente acontece mais frequentemente com sites de e-commerce.

A página falsa traz apenas alguns pequenos detalhes diferentes do site original, tentando **fazer com que a farsa passe despercebida**.

Esse tipo de golpe acontece durante todos os momentos do ano, mas se intensifica durante as **campanhas de grande apelo comercial**, como **Black Friday**, **Natal**, **Dia das Mães** e outras **datas comemorativas**, quando há um aumento significativo de compras on-line.

Redobre sua atenção!

Antes de informar seus dados pessoais, clicar em links ou realizar compras nestes sites, verifique o **endereço eletrônico** e confirme se as páginas possuem **certificação de segurança** “**https**”.

Golpe do código de acesso

Caso receba **códigos de acesso** por SMS ou aplicativos de mensagens, **não compartilhe com mais ninguém**.

Pessoas mal-intencionadas podem utilizar esse dado para **acessar** e **se apossar de suas contas** em redes sociais e outros aplicativos. Caso isso ocorra, os golpistas podem se passar por você, causando muitos problemas e gerando, inclusive, **prejuízos financeiros**.

Lembre-se!

Os códigos de segurança são **pessoais** e **intransferíveis**. Eles costumam ter 6 dígitos e servem como um **reforço de segurança** para ativar/acessar suas contas nos meios digitais.

O que a Petros faz pela segurança dos meus dados

Na Petros, a **proteção de dados** está incorporada à estrutura de **Governança**. Contamos com um setor específico para **Privacidade e Proteção de Dados**, ligado à Gerência de Governança, Riscos e Compliance.

Dispomos de **políticas específicas** que definem diretrizes que devem ser seguidas por toda a empresa e, periodicamente, realizamos **treinamentos**. Além disso, temos um **profissional dedicado** (DPO) a lidar com questões relacionadas à LGPD.

Para saber mais sobre a nossa atuação, ouça nosso podcast sobre proteção de dados e segurança da informação.

Ouça agora o nosso *podcast*

Nossos canais oficiais

Para se prevenir contra golpes é importante conhecer os canais oficiais da Petros. Confira quais são eles a seguir:

Canais digitais

- Portal Petros
- LinkedIn
- YouTube
- Spotify

Canais de Atendimento

Fale conosco
Disponível no Portal Petros ou pelo nosso aplicativo.

Atendimento online (chat)
Dias úteis, das 8h às 18h.
Para acessar, entre na Área do Participante com matrícula e senha Petros.

Central de Relacionamento - 0800 025 35 45
Dias úteis, das 8h às 20h.
Serviços automatizados 24h.

Proteção de dados e segurança da informação

PETROS