Golpes na internet

Orientações para aplicação do conteúdo formativo

MATERIAIS DISPONÍVEIS
- Apresentação em slides para oficinas e palestras;
- Este PDF com instruções e sugestões para o uso dos slides;
- Cartilha digital para o público 60+ (pode ser impressa).

Caro(a) oficineiro(a),

Este material orienta a aplicação do conteúdo da formação *Golpes na internet: avaliar mensagens para não se enganar*, módulo do programa EducaMídia 60+, voltado ao letramento midiático e informacional de pessoas com mais de 60 anos.

Aqui você encontrará um detalhamento do conteúdo pedagógico desenvolvido no formato de slides para discutir os tipos mais frequentes de golpes pela internet, ajudando seu grupo a identificá-los e, sobretudo, a avaliar criticamente qualquer tipo de mensagem apelativa à ação no mundo digital..

Assim, este módulo tem como **objetivos**:

- Conhecer as principais formas de golpes no mundo digital.
- Discutir comportamentos que colocam em risco os dados pessoais do cidadão, na internet.
- Explorar protocolos de análise e verificação de mensagens potencialmente golpistas.

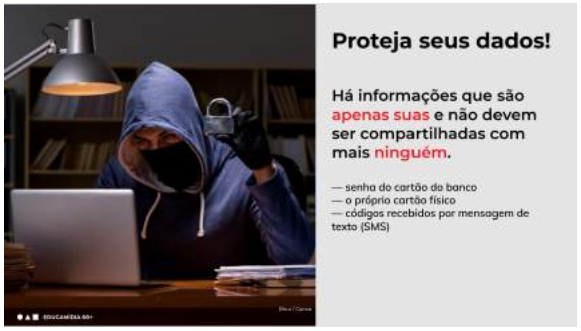
Assim, os **conteúdos** abordados nesta atividade serão:

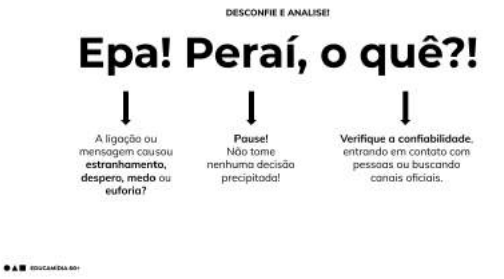
- Segurança na internet.
- Tipos frequentes de golpes na internet.
- Protocolos para avaliar mensagens potencialmente golpistas.

No quadro a seguir você encontra orientações acerca de cada um dos slides que compõem a apresentação deste módulo. Fique à vontade para customizar o conteúdo, conforme as necessidades do seu grupo e o nível letramento midiático

e digital, por exemplo, selecionando apenas alguns dos tópicos do material, em vez de aplicá-lo na íntegra. No final do quadro, você encontrará um gabarito para a atividade proposta nos últimos slides.

Estimamos que a oficina completa dure **entre 60 e 90 minutos**, a depender das intervenções do grupo ou da necessidade de tempo para a prática. Isso deve ser avaliado por você antes da realização do encontro. Boa atividade!

	**Golpes na internet** Dê as boas-vindas ao grupo, apresente-se (caso não conheça a turma) e explique os propósitos desta atividade. Ler os objetivos da formação, descritos acima, é uma forma de deixar claro o que se espera do encontro.
	Neste slide, afirmamos que o espaço da internet e os recursos digitais são benéficos e podem facilitar uma série de atividades do cotidiano. A intenção é deixar claro o objetivo da formação em demonstrar que os recursos digitais da internet podem e devem ser usados, mas com precaução. E para fortalecer essa habilidade de nos proteger no mundo digital é que esta formação foi pensada.
	**Proteja seus dados!** Neste slide, queremos reforçar a importância de manter em sigilo algumas informações que são privadas e que não devem ser repassadas a ninguém sob nenhum pretexto, como: senha de cartões e contas, cartões físicos ou códigos recebidos por mensagens de texto.
	**Desconfie!** Aqui, nosso intuito é chamar a atenção para situações em que devemos desconfiar da intenção do outro em nos abordar por mensagem em aplicativos, mensagem de texto ou contato telefônico. Leia os tópicos apresentados no slide e reforce que todas essas situações são motivos para desconfiar. Mesmo se recebermos mensagens de pessoas conhecidas, estas podem ter tido suas informações roubadas por golpistas e

	estes se passam por nossos contatos para pedir dinheiro ou nossas informações pessoais. Não explique aqui como esses roubos ocorrem, Trataremos disso mais adiante, nos próximos slides.
	**Fique esperto(a)!** Aqui apresentamos uma forma de analisar abordagens suspeitas, como as listadas no slide anterior. Explique ao seu grupo que esse quadro apresenta três passos que toda pessoa abordada pode seguir para evitar ser enganada. Na primeira coluna destacamos algumas perguntas que ajudam a refletir sobre a abordagem em si. Basta ler as perguntas. Na segunda coluna, chamamos a atenção para a necessidade de agir caso a abordagem gere desconfiança. Essa ação envolve entrar em contato com a pessoa que (supostamente) nos abordou. Reforce no grupo a necessidade de procurar pela pessoa em questão por outro canal que não aquele por meio do qual fomos abordados. Vale apresentar este exemplo: se um amigo ou parente pede dinheiro a você pelo WhatsApp, telefone para ele ou mande mensagem por uma rede social, como Facebook ou Instagram. Se a abordagem for por essa rede social, procure-o pelo WhatsApp. Se ainda assim estiver desconfiado, peça para que a pessoa mande um áudio, para que seja possível certificar-se com quem estamos falando. Na última coluna, apresentamos o que podemos fazer caso constatemos que a abordagem se trata de um golpe.
	**Epa! Peraí, o quê?!** Este é outro protocolo para verificar se a abordagem é realmente confiável. Diga ao seu grupo que, inicialmente, no **“Epa!”**, refletimos sobre a mensagem ou ligação recebida e o que ela nos desperta: estranhamento, desespero, medo, euforia. A segunda etapa, o **“Peraí”** reforça a necessidade de refletir sobre a mensagem ou ligação antes de tomar qualquer atitude. Por fim, a terceira etapa, **“o quê?!”** nos incentiva a verificar, agindo conforme a coluna “Verifique”, no protocolo anterior, nos orienta.

	**Phishing** Neste slide, apresentamos o conceito de phishing (lê-se “fíxin”), que consiste em um ataque virtual por meio de links a partir dos quais os golpistas têm acesso a dados privados e que podem ser espalhados por diversos meios digitais, como e-mail, WhatsApp ou SMS. É a partir desse tipo de ataque que é possível clonar WhatsApp, roubar listas de contato ou fazer compras online, a partir de dados bancários.
	**Clonagem do WhatsApp** A partir daqui, até o slide 15 (sobre Site impostor), explicaremos como funcionam alguns golpes na internet. Este slide explica em que consiste a clonagem de WhatsApp. O primeiro tópico apresenta como o golpista se apresenta para a vítima, isto é, para a pessoa de quem clona o aplicativo. O segundo tópico explica como a clonagem ocorre: a pessoa que tem seu WhatsApp clonado informa um código para o golpista que, provavelmente, a contatou por telefone. No entanto, reforce que a clonagem também pode acontecer quando clicamos em links enviados por contatos desconhecidos. O terceiro tópico diz como agem os golpistas após terem efetuado a clonagem.
	**Clonagem do WhatsApp** Aqui, demonstramos como aplicar o protocolo “Epa! Peraí, o quê?!” para evitar ser vítima de um golpe por WhatsApp em que somos abordados por um contato que nos pede dinheiro. Explique isso antes de ler os tópicos. No **“Epa”**, devemos refletir sobre a abordagem. Assim, vale a pena parar para pensar se a pessoa em questão costuma pedir dinheiro e se tem intimidade para isso. No **“Peraí”**, a ideia é verificar se de fato é um amigo, colega ou parente que está pedindo dinheiro. Vale a pena ligar para a pessoa ou mandar mensagem por outra rede social, ou até mesmo por e-mail. Vale a pena dizer ao seu grupo que se no contato telefônico ou por rede social chegar à conclusão de que, de fato, era, de fato, um amigo ou familiar fazendo o pedido, basta esclarecer que preferiu ligar

	por segurança, pois, hoje em dia, muitas pessoas têm seus aplicativos clonados. Por fim, no **“o quê?!”**, basta dizer que se na conversa com a pessoa, chegar à conclusão de que era golpe, deve-se bloquear o contato no WhatsApp.
	**SMS impostor** Neste slide, introduzimos outro tipo de golpe. Aqui, apresentamos um exemplo de mensagem de texto (SMS), por meio do qual golpistas enviam um link. Chame a atenção, junto ao seu grupo, para a mensagem de SMS: o golpista se passa por um banco e pede que a vítima clique no link enviado para, supostamente, atualizar seus dados. Esclareça que operadoras financeiras não contatam clientes por SMS para pedir atualizações. Instrua seu grupo a não clicar no link e a bloquear o número a partir do qual a mensagem foi enviada.
	**SMS impostor** Neste slide, listamos possíveis conteúdos de mensagens impostoras por SMS. O primeiro tópico (Falsa atualização) explica que uma estratégia adotada é simular a necessidade de atualizar, com urgência, informações, sob o risco de ter uma conta encerrada, conforme exemplo apresentado no slide anterior. O golpista pode ainda se passar por uma operadora financeira, que deseja confirmar uma compra ao clicar num link. Ele pode ainda se passar por uma operadora financeira que tem uma oportunidade imperdível. Reforce que ao abrirmos um link enviado por um SMS impostor, **os contatos do celular podem ser roubados.** Ao possuí-los, os golpistas podem, por telefone, abordar nossos conhecidos, com o intuito de roubar seus dados, também se passando por funcionários de operadoras financeiras e até por sequestradores.

	**Roubo da lista de contatos** Neste slide, novamente, lembramos o protocolo “Epa! Peraí, o quê?!” para ser aplicado em situações como as listadas no slide anterior (compra falsa, falso investimento ou falso sequestro), seja por SMS ou telefone. Leia com seu grupo as informações do slide e as explique, conforme abaixo: - **Epa!:** o contato telefônico ou SMS me amedrontou ou pediu minha senha. Desconfio! - **Peraí:** caso se apresentem, numa chamada telefônica, como um funcionário de uma operadora financeira, agradeça o contato e diga que você mesmo irá entrar em contato ou que irá verificar os lançamentos de suas últimas compras no aplicativo do seu cartão. Se for um suposto sequestrador, encerre a chamada e entre em contato por telefone com seu familiar ou amigo. - **O quê?!:** ao perceber a fraude, bloqueio o número.
	**Perfil falso (fake)** Aqui, exploramos mais um tipo de golpe. Destaque que golpistas podem forjar o perfil de uma marca, loja, instituição e até mesmo de outra pessoa para pedir dinheiro aos contatos e seguidores, por exemplo. Perfis falsos de marcas ou lojas criam promoções e vendem produtos falsos. Há ainda perfis falsos de hospedagens, que oferecem falsas reservas. Diga ao seu grupo que, nesses casos, é importante usar buscadores para encontrar sites oficiais dessas empresas ou organizações e, por meio destes, verificar os perfis das redes sociais. Fazendo essa busca, será possível confirmar se o perfil que seguimos é, de fato, o perfil oficial de lojas, marcas, pessoas e hotéis.

Golpe da maquininha

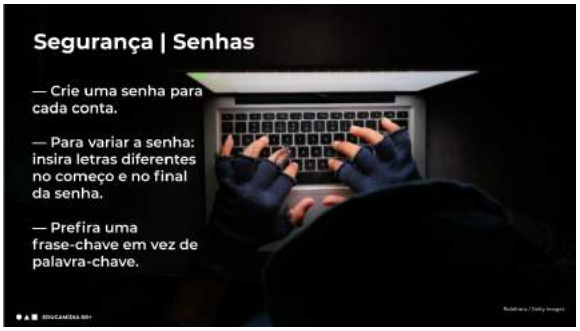
Aqui, apresentamos outro tipo de golpe: o golpe da maquininha. Diga ao seu grupo que esse tipo de golpe não é pela internet, mas ocorre de modo presencial. No entanto, o golpista pode alegar que houve uma falha no pagamento online e, por isso, deseja cobrar a compra pelo cartão. Nesse contexto, passam valores superiores ao valor alegado, sem que isso fique evidente para a vítima. Esclareça o seu grupo que compras feitas pela internet são confirmadas por e-mail ou WhatsApp e que não há possibilidade de um produto ser entregue, cuja compra não tenha sido efetivada virtualmente. Caso haja alguma abordagem desse tipo, devemos dizer ao entregador que recebemos a confirmação do pedido e, sem isso, ele sequer estaria fazendo a entrega.

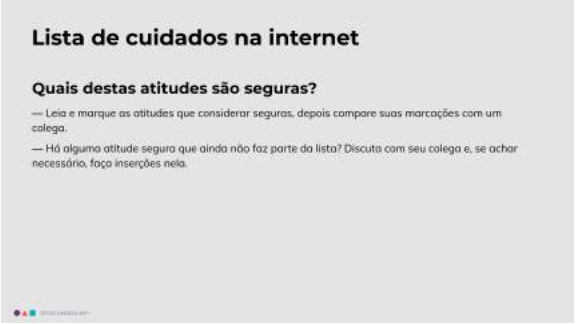
Site impostor

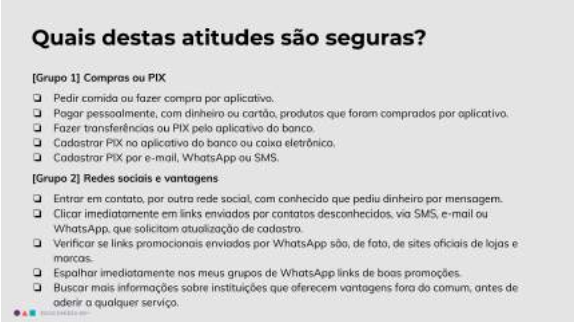
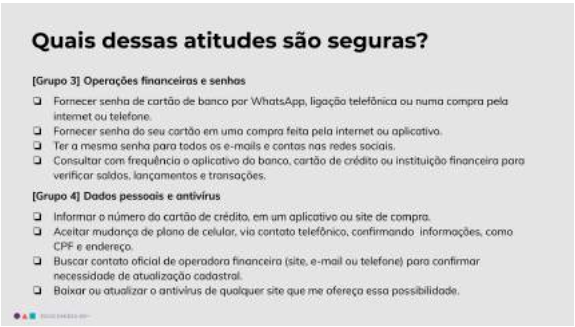
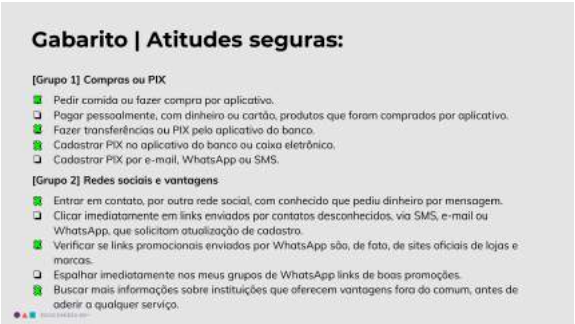
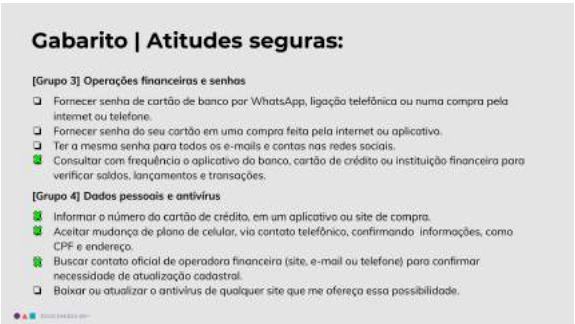
Neste slide, abordamos o último tipo de golpe: site impostor. Explique ao seu grupo que esse tipo de site finge ser de instituições verdadeiras, copiando sua aparência e identidade visual. Sites impostores têm nomes parecidos aos sites que querem imitar, mudando pequenos detalhes, como no exemplo, em que um site impostor imita o "m" de "magazine", forjando sua aparência com a junção de um "r" e um "n", por exemplo. No último exemplo, diga que sites impostores também disparam e-mails, cujo endereço também se assemelha ao de um site oficial e pode passar despercebido por leitores menos atentos.

Por fim, chame a atenção do seu grupo para a imagem do slide e diga que sites que não seguros aparecem com o cadeado aberto no navegador e, geralmente, os navegadores (como Google ou FireFox) alertam o usuário caso estes estejam prestes a acessar um site dessa natureza. No entanto, não é possível apenas depender do alerta do navegador, que nem sempre detecta sites impostores. É preciso ter atenção e, na dúvida, abrir um buscador para encontrar sites oficiais e compará-los àqueles que foram enviados para nós.

	**Segurança** Ao contrário da imagem do slide anterior, sites seguros aparecem no navegador com a imagem do cadeado fechado, como demonstra a imagem do slide. Para garantir essa identificação, no entanto, é preciso manter o antivírus atualizado. Mas é importante destacar o seguinte: o cadeado significa que a informação irá apenas trafegar de forma segura de uma ponta a outra, não significa que o site é legítimo, então não necessariamente ter HTTP é sinônimo de segurança para pessoa, apenas para os dados.
	**Segurança | E-mail** Aqui, damos uma dica para evitar abordagens golpistas por e-mail: ter um e-mail apenas para cadastro em sites ou aplicativos de compra, pois evita colocar em risco uma conta usada para atividades mais cotidianas.
	**Segurança | Redes sociais** Aqui, sugerimos que os participantes possam refletir sobre quem pode visualizar suas publicações nas redes. No Facebook, por exemplo, é recomendável não deixar suas publicações públicas, especialmente as que revelam informações sobre nossa vida pessoal, conforme demonstra o quadro abaixo do primeiro tópico, que diz respeito ao Facebook. No Instagram, é possível manter a conta fechada e autorizar que apenas pessoas conhecidas nos sigam. O segundo tópico fala sobre rever postagens antigas para avaliá-las se elas revelam aspectos importantes da nossa intimidade, o que também reforça a nossa segurança. Se entender que há informações que não queremos compartilhar com estranhos, é possível restringir sua visualização apenas aos amigos.

<table>
<tr>
<td> 
</td>
<td>Segurança | Senhas
Aqui, damos dicas de segurança quanto às senhas. No primeiro tópico, reforçamos a importância de não as reutilizar, isto é, não ter a mesma senha para várias contas, pois se a senha de uma conta for descoberta, as demais contas ficam comprometidas. Dessa forma, no segundo tópico, damos uma dica de como variar uma senha: basta acrescentar uma letra diferente no início e no final de uma mesma senha para diferenciá-la da de outras contas. Nesse sentido, reforce que a letra escolhida pode ter relação com o nome do site em que nos cadastramos ou com a finalidade da conta. Por exemplo: um e-mail para finalidade profissional pode ter como letra inicial “P” e letra final “L”. O meio da senha pode ser comum a de outras contas, como a conta do Facebook, pode ter como letra inicial “F” e a final “K”. Por fim, recomendamos que em vez de palavras, possamos criar frases-chave, que complexificam a senha, tornando-a mais forte, com mais caracteres.</td>
</tr>
<tr>
<td> 
</td>
<td>Se cair...
Neste slide, orientamos o grupo a tomar providências básicas caso seja vítima de algum golpe na internet.
- Caso perceba compras lançadas em seu cartão de crédito ou saques realizados, é preciso avisar o banco ou operador financeiro com urgência, a fim de cancelar os cartões para que o golpista não siga comprando ou fazendo saques. Compras não reconhecidas pelo titular do cartão também são canceladas. Saques, no entanto, não são ressarcidos.
- Oriente seu grupo, ainda, a registrar boletim de ocorrência e fazer denúncia no site do Procon ou Ministério da Justiça.</td>
</tr>
<tr>
<td> 
</td>
<td>Nunca...
Neste slide, destacamos atitudes que nunca devem ser tomadas. Nesse sentido, relembre o grupo:
- Bancos ou outras operadoras e plataformas não precisam de nossas senhas para resolver problemas. Não devemos passá-las a ninguém.</td>
</tr>
</table>

	- Não devemos deixar nossas senhas anotadas em blocos de nota no celular nem em cadernetas que podem ser acessadas facilmente por outras pessoas. - Os códigos que recebemos por SMS servem para confirmar operações. Se esses códigos caem nas mãos de golpistas, eles podem se passar por nós. - Caso alguém peça informações por e-mail, WhatsApp ou SMS dizendo que a finalidade é cadastrar o PIX, desconfie. PIX é cadastrado somente pelo aplicativo do banco ou na agência bancária.
	**Sempre...** Neste slide, basta ler os tópicos que reforçam comportamentos seguros na internet.
	Por fim, ressaltamos a importância de sempre avaliar as mensagens recebidas a partir dos protocolos que conhecemos neste módulo. Reforce que sempre há novos golpes, mas que é possível escapar deles desconfiando do que é fora do comum e de abordagens urgentes, que pedem uma atitude imediata, e verificando se a informação apresentada na abordagem é verdadeira ou não. Caso constatemos o golpe, alertamos as pessoas envolvidas, bloqueamos o contato (se for o caso) e denunciamos.
	**[ATIVIDADE PRÁTICA]** Como atividade prática, propomos um check-list de atitudes rotineiras na internet. O desafio é que seu grupo possa marcar apenas as atitudes que consideram seguras. Organizamos essas atitudes em 4 grupos. Essa atividade pode ser realizada individualmente ou em pequenos grupos em que os participantes dialogam sobre cada um dos itens da lista e, juntos, assinalam as que considerarem seguras, de comum acordo. Aplique a atividade

	conforme o perfil e desejo do grupo. Mas após analisarem todos os pontos da lista e escolherem os que se referem a atitudes seguras, os participantes devem comparar suas respostas com outros participantes ou grupos. Nesse momento, deixe-os livres para circular pelo ambiente e dialogar com seus colegas sobre suas escolhas. Estimamos que o tempo de aplicação da atividade deve ocorrer entre 15 e 30 minutos.
 	Caso deseje ler com o seu grupo cada uma das atitudes que compõem as 4 listas, especialmente se o grupo for pequeno, você pode utilizar estes slides e realizar a atividade com os participantes. Essa mesma lista está disponível em um Google Formulário, caso queira disponibilizá-lo para que os participantes façam a marcação em uma plataforma digital, que após a submissão das respostas, dará um feedback. Você ainda pode imprimir e adaptar a lista, disponível para cópia, neste Google Doc.
 	**Gabarito** Nestes dois slides, revelamos as respostas corretas. Fizemos uma marcação verde nos itens das listas que representam atitudes seguras na internet. Reproduzimos abaixo os feedbacks disponíveis no formulário para discutir as escolhas feitas pelos participantes:

Feedbacks para as respostas corretas e incorretas:

[Grupo 1] Compras e PIX

Feedback das respostas corretas:
Muito bem! Pedir comida ou fazer compra por aplicativo e fazer transferências ou PIX pelo aplicativo do banco e cadastrar o PIX no caixa eletrônico ou aplicativo do banco são atitudes seguras.

Feedback das respostas incorretas:
Cuidado! PIX só deve ser cadastrado no aplicativo do banco, caixa eletrônico ou dentro da agência bancária. Pagar pessoalmente, com dinheiro ou cartão, produtos que foram comprados por aplicativo é golpe! A confirmação da compra aparece no aplicativo onde a compra foi efetuada e é enviada por e-mail, WhatsApp ou SMS.

[Grupo 2] Redes sociais e vantagens

Feedback das respostas corretas:
Muito bem! Devemos SEMPRE verificar quando algum conhecido nos pede dinheiro ou quando uma suposta instituição entra em contato nos oferecendo uma boa oportunidade ou divulgando promoções.

Feedback das respostas incorretas:
Cuidado! Antes de clicar imediatamente em links enviados por contatos desconhecidos e de espalhar promoções, que tal verificar a procedência da informação? Não tome atitudes precipitadas, induzido por falsas urgências ou por supostas boas oportunidades. Gaste uns minutos para checar se o link enviado é, de fato, confiável.

[Grupo 3] Operações financeiras e senhas

Feedback da resposta correta:
Muito bem! Consultar com frequência o aplicativo do banco, cartão de crédito ou instituição financeira para verificar saldos, lançamentos e transações é muito importante. Caso ocorra alguma compra que você não tenha feito, comunique imediatamente sua operadora financeira e solicite o cancelamento da compra e do cartão, que pode ter sido clonado.

Feedback das respostas incorretas:
Ao comprar por telefone, internet ou WhatsApp devemos apenas informar os dados do cartão, mas NUNCA A SENHA. Com ela, outras pessoas podem fazer compras ou saques passando-se você. Tome cuidado! Além disso, não é seguro manter a mesma senha para todas as nossas contas de e-mail e redes sociais. Diversifique-as com letras diferentes para cada conta, no começo e no final da senha que costuma usar.

[Grupo 4] Dados pessoais e antivírus

Feedback das respostas corretas:

Muito bem! Alguns dados pessoais podem ser fornecidos durante a compra ou atualização de planos, como:
- Número do cartão.
- Endereço.
- Parte do número do CPF.
Você faz muito bem em entrar em contato com sua operadora financeira para saber se, de fato, é necessária qualquer atualização cadastral, que não é algo urgente. Se pedirem para que você atualize suas informações imediatamente, com ameaça de cancelar sua conta, por exemplo, não caia nessa.

Feedback da resposta incorreta:
Cuidado! Não devemos baixar antivírus de qualquer site. Consulte profissionais de Tecnologia da Informação sobre sites a partir dos quais podemos obter ou atualizar esse recurso com segurança.