

Cartilha

Segurança e

Proteção de Dados



A Unimed Blumenau está sempre trabalhando para manter a segurança e privacidade dos dados de seus beneficiários. Por isso, também preparamos algumas **dicas de cuidados para você adotar no seu dia a dia**. Confira a seguir.

CUIDADOS COM BOLETOS

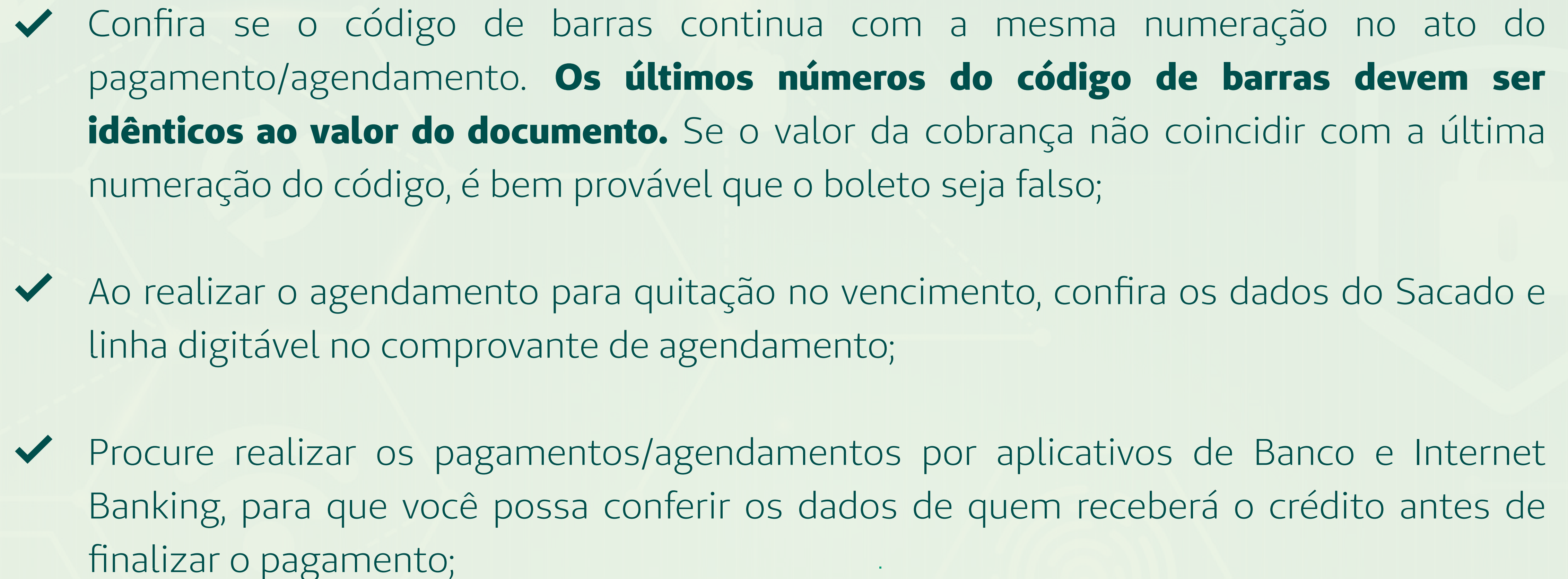
Disponibilizamos os boletos das seguintes formas:


- ✓ Fisicamente (enviado à residência do beneficiário)
- ✓ Via E-mail
- ✓ Portal do Beneficiário
- ✓ Aplicativo Unimed Cliente
- ✓ Por meio do WhatsApp

Mesmo com todo o cuidado, as fraudes em boletos têm sido cada vez mais comuns, por isso **é importante ter alguns cuidados na hora de realizar o pagamento do boleto bancário, para não cair em uma armadilha:**

- ✓ Confira com atenção os dados do destinatário, verificando se são realmente para a empresa que você deseja realizar o pagamento. **Os boletos em nome da Unimed Blumenau apresentam a Razão Social Unimed Blumenau Cooperativa de Trabalho Médico e CNPJ 82.624.776/0001-47;**
- ✓ Verifique se os dados estão corretos, confira nome completo (sem abreviações), CPF, endereço, código de carteirinha e valores;



- 
- ✓ Confira se o código de barras continua com a mesma numeração no ato do pagamento/agendamento. **Os últimos números do código de barras devem ser idênticos ao valor do documento.** Se o valor da cobrança não coincidir com a última numeração do código, é bem provável que o boleto seja falso;
 - ✓ Ao realizar o agendamento para quitação no vencimento, confira os dados do Sacado e linha digitável no comprovante de agendamento;
 - ✓ Procure realizar os pagamentos/agendamentos por aplicativos de Banco e Internet Banking, para que você possa conferir os dados de quem receberá o crédito antes de finalizar o pagamento;

- 
- ✓ Evite realizar a impressão de boleto. É muito comum golpistas utilizarem softwares específicos para conseguir fraudar o documento no momento da impressão. Caso você opte por imprimir, é importante manter o antivírus do computador sempre atualizado para evitar cair nesse golpe;
 - ✓ Não pague boletos com descontos/abatimentos sem que a negociação tenha ocorrido com a Unimed;
 - ✓ Se possível, habilite o sistema de recebimento e cobrança bancária DDA (Débito Direto Autorizado). O DDA é um sistema desenvolvido para ser uma plataforma em que o cliente possa receber seus boletos para pagamento de forma eletrônica, podendo ser acessados através da internet, caixas eletrônicos e telefone, acabando com a necessidade do envio de boletos. Portanto, o sistema DDA passa a ser mais seguro para evitar boletos fraudulentos;

- ✓ Evite pagar boletos em casas lotéricas ou direto nos caixas dos bancos. Dificilmente o atendente irá lhe questionar ou notar que o boleto sofreu alguma alteração, portanto procure você mesmo observar com atenção;
- ✓ Com o intuito de combater os casos de fraudes de boletos, a Unimed Brasil disponibiliza em seu site os canais oficiais das operadoras para segunda via de boletos. Basta preencher no formulário o estado e cidade, e selecionar sua Unimed. Acesse em: unimed.me/2via;
- ✓ Para emissão de segunda via de boletos da Unimed Blumenau, acesse o Portal do Beneficiário (portal.unimedblumenau.com.br/login), o App Unimed Cliente, solicite através do WhatsApp 47 99901 0459 ou entre em contato através do 0800 647 0026. **Não possuímos outros canais para emissão de segunda via de boleto, fique atento!**

ATENÇÃO:

Utilizou seu cartão de crédito ou débito para realizar uma compra na Internet? Confira o extrato do seu cartão logo em seguida, garantindo que foi cobrado o valor correto e pago para a empresa certa. **Não entregue o cartão para o funcionário que está realizando a cobrança, pois esse cartão poderá ser trocado ou os dados anotados, principalmente o código de segurança.**

Muitos bancos possuem aplicativos com a funcionalidade de Cartão Virtual. Não deixe de utilizar o benefício. Na maioria dos casos, quando você faz uma compra na internet, utilizando o número do cartão virtual, quando terminar a transação, esse cartão deixará de existir com aqueles dados. Mesmo se alguém pegar as informações, não conseguirá mais utilizar.





BOAS PRÁTICAS **PARA USO DO** **WHATSAPP**

Por ser tão utilizado, o WhatsaApp se tornou alvo frequente para fraudes. Então é importante ficar atento a algumas informações.

**Caso receba mensagens suspeitas ou indesejadas,
você pode bloquear o número ou denunciar como spam.**

A Unimed Blumenau possui serviço de atendimento
através do WhatsApp pelo seguinte número:

 **47 99901 0459**

 **0800 647 0026**

Nossas Unidades também possuem WhatsApp
para atendimento, sempre confirme o contato!

Confira outras dicas importantes quanto ao uso do seu WhatsApp.

VERIFICAÇÃO EM DUAS ETAPAS

Com a verificação em duas etapas, sempre que você precisar instalar o WhatsApp em um novo aparelho, será necessário informar um código de registro, enviado por SMS. Esse código é uma ferramenta de segurança desenvolvida para evitar que uma mesma conta seja instalada em dois celulares, o que garante a privacidade das mensagens.

Para ativar essa verificação no WhatsApp, vá até a aba **Configuração > Conta**. Em seguida, escolha a opção **Confirmação em duas etapas**. Você precisará cadastrar uma senha (PIN) de seis dígitos e informar um endereço de e-mail para recuperar o código, caso o esqueça.

CUIDADO:

Há pessoas mal-intencionadas com estratégias para descobrir o código de verificação do seu WhatsApp, roubar sua conta e aplicar golpes em seu nome. O processo geralmente é feito por ligação telefônica, mas fique atento a outras formas de contato.

O farsante diz que trabalha para uma empresa conhecida, como grandes lojas, bancos e companhias telefônicas, e conta alguma história. No meio da conversa, ele pede um código recebido por SMS. Se você não perceber que se trata de um golpe, irá informar o código de registro do seu WhatsApp, permitindo o acesso à sua conta.



SENHA NO WHATSAPP

Sabia que é possível colocar senha nos aplicativos instalados no seu smartphone? Assim, além do código para desbloquear o aparelho, será necessário informar a senha para abrir o APP. Essa medida é mais uma forma de proteção para que pessoas mal-intencionadas não acessem suas informações pessoais durante uma tentativa de fraude.

Muitos aparelhos contam com essa funcionalidade e a configuração dependerá do seu modelo e do sistema operacional. Geralmente, a função de bloqueio fica na aba “Segurança” ou “Privacidade”. Se o seu celular não tiver essa função, você pode baixar um app para criar um bloqueio adicional para o WhatsApp, para aplicativos de bancos e de fotos, e-mail, entre outros. Além disso, lembre-se de manter seu aplicativo atualizado para ter acesso aos aprimoramentos de segurança.

ATENÇÃO AOS LINKS

Sempre desconfie de links que recebeu pelo WhatsApp de números desconhecidos! Os cibercriminosos têm muitas técnicas para capturar dados de usuários e aplicar golpes.

Não clique em links duvidosos e sempre desconfie de mensagens que oferecem grandes descontos, produtos e serviços gratuitos, entre outras ações “imperdíveis”. Essas estratégias são utilizadas por hackers para coletar dados dos usuários. Isso pode ser feito por meio do preenchimento de formulários fakes ou com a instalação de programas espiões no dispositivo, o que permite o acesso aos dados que estão nele, incluindo mensagens do WhatsApp.



SESSÕES ATIVAS NO WHATSAPP WEB

Muitos usuários utilizam o WhatsApp pelo navegador, mas apesar da funcionalidade trazer certa praticidade à rotina, também requer mais atenção dos usuários.

Sempre que finalizar a utilização do WhatsApp Web, verifique as sessões ativas para saber quais dispositivos estão conectados. Para fazer isso, entre na sua conta pelo celular, vá até a aba “WhatsApp Web” ou “Aparelhos Conectados”. Se não reconhecer algum deles, clique para encerrar a sessão. Procure fazer isso com frequência.

GOLPES ATRAVÉS DAS REDES SOCIAIS

É preciso ter muito cuidado com o que compartilhamos, pois simples publicações podem fornecer muitas informações sobre você para os golpistas.

Desconfie sempre de mensagens com erros gramaticais ou de grafia. Ofertas reais, de empresas confiáveis geralmente possui setores específicos para a criação do conteúdo, que dificilmente conterá erros grotescos.





Não acesse links de origem desconhecida ou mensagens que contenham endereços específicos para clicar. Desconfie também daquele influenciador famoso, que está divulgando uma oferta muito boa. Atualmente, até os mais conhecidos no mundo da internet estão auxiliando nos golpes ou foram vítimas e acabaram tendo sua rede social clonada ou hackeada.

Recebeu um e-mail que caiu no spam ou lixo eletrônico? Avalie se não é golpe, o próprio provedor de e-mail já possui tecnologias para detectar mensagem fraudulentas. **Não responda a pedidos desconhecidos de compartilhamento de dados pessoais como senhas, contas de banco, cartões de crédito e débito, CPF ou RG, entre outros.**

BOAS PRÁTICAS COM SENHAS

Por vezes é chato a utilização de senhas complexas, porém essa é ainda a forma mais eficiente de autenticação, garantindo que apenas pessoas autorizadas possam acessar serviços como e-mails, portais, aplicativos, etc.

Uma senha segura deverá conter, no mínimo, oito caracteres com letras (maiúsculas ou minúsculas), números e caracteres especiais, devendo conter no mínimo três dos quatro requisitos. Além disso, procure trocar suas senhas a cada 60 dias e evite utilizar senhas repetidas ou semelhantes às anteriores e tente manter um padrão de, pelo menos, três senhas diferentes para utilizar em todos os seus aplicativos e sites. Não empreste suas senhas para ninguém, e se isso for necessário, após o uso, troque imediatamente a combinação.

Evite senhas com o nome relacionado à sua conta ou dados pessoais, duplicando, invertendo, acrescentando um número, ou qualquer variação do mesmo, como partes do próprio nome, endereço, data de nascimento, placa do carro, carteira de identidade, CPF, nome da(o) namorada(o), do cachorro, etc. É fácil alguém conseguir esses dados e acabar adivinhando a senha por tentativa e erro.

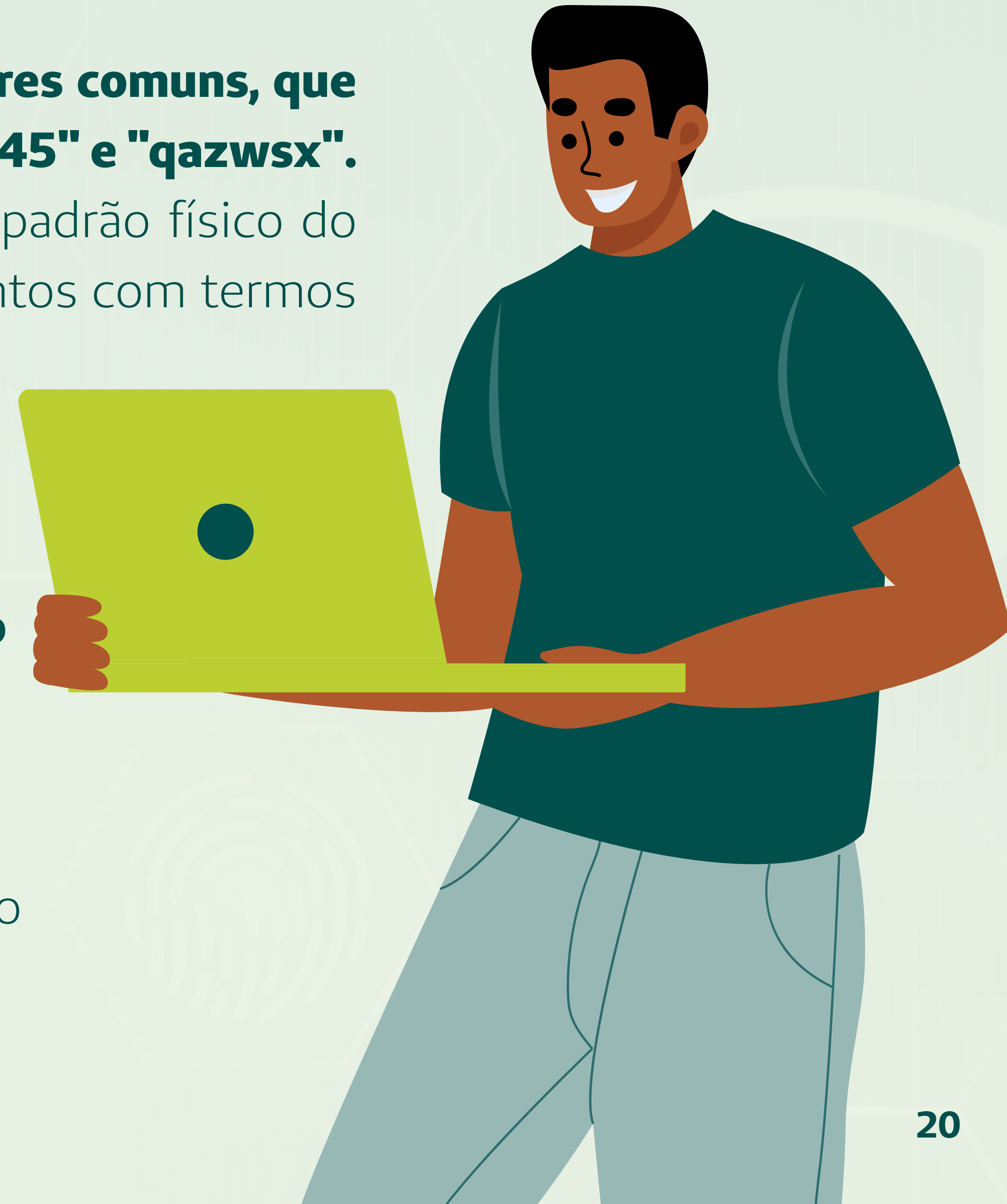
Também é indicado não usar nomes próprios. Nomes de pessoas, cidades e países, por exemplo, já estão em listas ou dicionários eletrônicos. Facilita muito o trabalho de adivinhar a senha por tentativa e erro.



Sugere-se, ainda, não utilizar sequências de caracteres comuns, que facilmente serão decifradas, como por exemplo "12345" e "qazwsx".

Essa última parece mais complicada, mas segue um padrão físico do teclado. Existem listas ou dicionários eletrônicos prontos com termos de áreas específicas, que são comumente utilizados como senhas. Seja o mais criativo possível.

Por fim, evite modificar palavras apenas substituindo "i" por "1", "o" por "0", "e" por "3", etc. Essa técnica pode ser utilizada em combinação com outras, mas deve ser evitado usar apenas ela, pois esse truque já é bastante conhecido e cada vez mais está se tornando facilmente descoberto.





Mantenha seu sistema, seja de um computador ou smartphone, atualizado e livre de malwares. Muitos desses softwares maliciosos podem capturar as suas senhas e seus dados, tornando inúteis todos os cuidados que você teve até agora, e colocando em risco todas as suas contas.

A Unimed Blumenau possui áreas específicas para garantir Compliance, Segurança e Proteção de Dados. Trabalhamos ativamente para evitar golpes, mal uso das informações, incidentes e tornar seguro os processos da Cooperativa.

Saiba mais em: unimed.coop.br/site/web/blumenau/governanca.



VOCÊ ACOMPANHA AS **PÁGINAS DA UNIMED BLUMENAU** **NAS REDES SOCIAIS?**

Estamos sempre compartilhando conteúdos sobre saúde, bem-estar, qualidade de vida, benefícios dos nossos planos, dicas de segurança e proteção de dados.

 **@unimedblumenau**

 **/unimedbnu**

 **/unimed-blumenau**

 **@unimedblumenau**

Unimed 
Blumenau