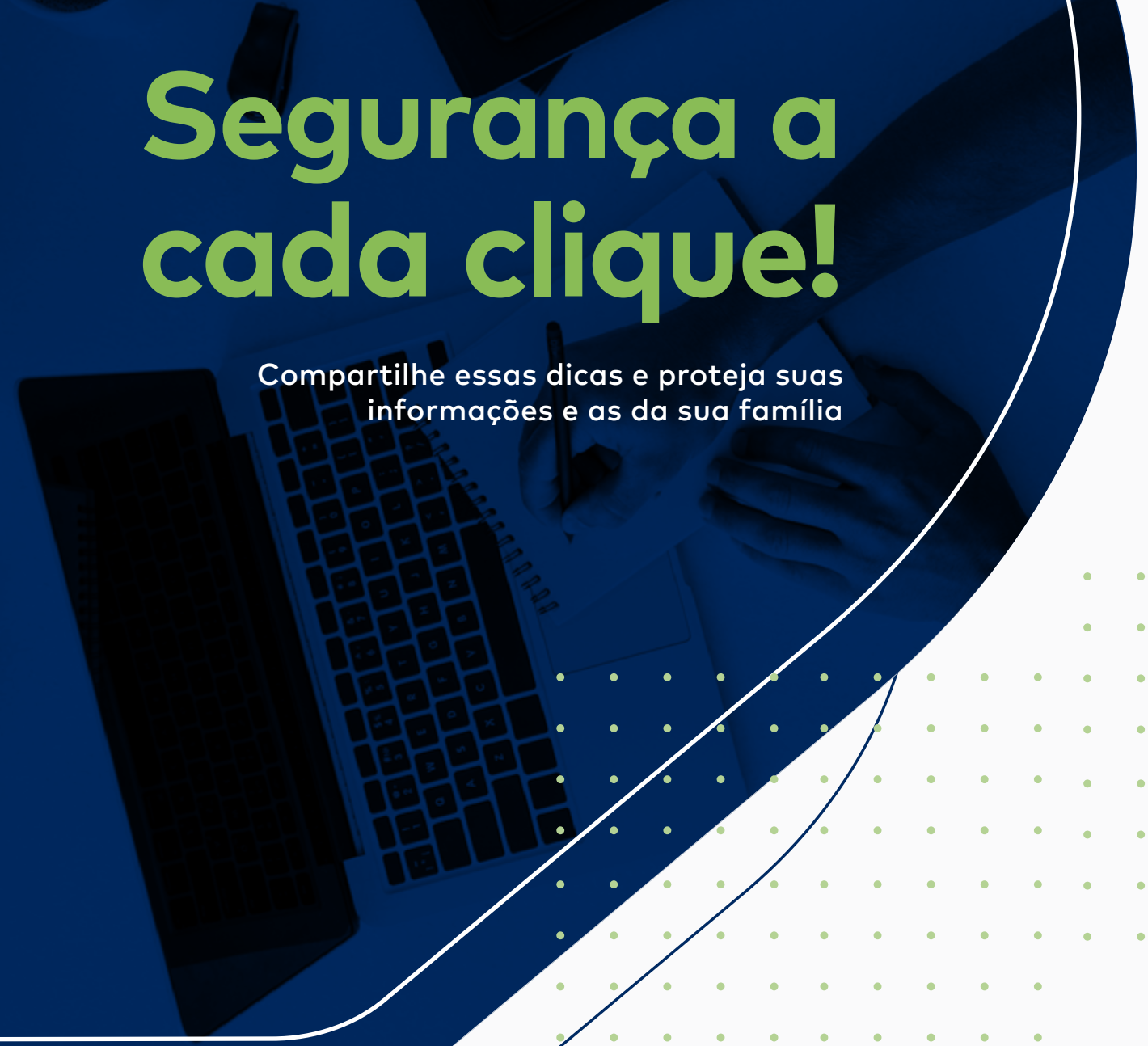


Segurança a cada clique!

Compartilhe essas dicas e proteja suas informações e as da sua família

agibank®

O que é essa cartilha?

Segurança a cada clique! é um material com informações e dicas práticas pra você ter hábitos seguros em ambientes físicos e digitais. Hábitos que deveriam ser compartilhados por todos, por isso sinta-se à vontade para dividir nossa cartilha com seus familiares e amigos.

Alguns descuidos com nossas informações podem trazer muitos prejuízos. Nosso objetivo é garantir que você conheça os perigos, se proteja dos riscos e compartilhe os ensinamentos aprendidos. Fazendo com que mais pessoas percebam a importância da segurança da informação no cotidiano.

agibank®

Índice

1 Você conhece os **perigos** da vida digital?

Todos os dias, milhares de informações são trocadas pela internet. Esses dados servem para pessoas mal-intencionadas aplicarem golpes. Provavelmente você já recebeu um e-mail falso, SMS suspeito ou até mesmo um trote telefônico. Se não aconteceu com você, com certeza conhece alguém que já tenha passado por isso, certo?

Com os cuidados sugeridos nesta cartilha, vai ser muito difícil você cair em um desses golpes no futuro.

Eu consigo **identificar** mensagens maliciosas?

Fique sempre atento a todas as mensagens que receber!

- Conheça todos os seus contatos;
- Lembre se já passou seu e-mail ou telefone para quem enviou as mensagens;
- Observe se o endereço de e-mail está correto e se a mensagem possui erros de português;
- Observe também o conteúdo das mensagens, quando maliciosas costumam ser impessoais (sem citar seu nome) e urgentes (ex.: "faltam poucos dias!").

Como não se tornar uma **vítima!**

O e-mail é uma ferramenta muito útil, mas muitas pessoas utilizam a mesma conta tanto para o trabalho quanto para o pessoal. Se alguém conseguir seus dados de acesso, também consegue ler suas mensagens pessoais e profissionais, podendo enviar golpes para seus contatos. Por isso:

Cuidado com URLs encurtadas (Ex: https://bitly.com/...);

Nunca passe senhas e dados pessoais, como números de documentos;

Cuidado com downloads que podem infectar seu computador;

Não repasse correntes, outras pessoas podem cair em golpes.

Tenha **consciência** de todos os seus passos...

Além das mensagens, seu celular ou computador também podem ser infectados se você entrar em sites suspeitos.

Páginas seguras geralmente começam com HTTPS, um protocolo que protege toda a troca de informações do site com seus visitantes.

Mas só isso não é suficiente. Cuide sempre também:

- Se antes da URL aparece um **símbolo de cadeado**;
- Se o domínio está **realmente correto**, com as terminações ".com" ou ".com.br";
- Se surgem **pop-ups suspeitos** na tela ou se **downloads automáticos** são realizados;
- Se pedem **dados pessoais** para liberar seu acesso.

2 Em quanto tempo **descobrem** suas senhas?

As senhas comprovam que você realmente é o dono de uma conta e tem permissão para estar no ambiente desejado. Para que ninguém se passe por você, é importante ter em mente que:

Suas senhas precisam ser diferentes entre si;

Só você pode sabê-las. Então não as diga a ninguém;

E não as anote em lugares de fácil acesso, como o bloco de notas do seu celular.

Senha **forte**, mente tranquila

"Tentativa e erro" é uma das maneiras para descobrir senhas. Por isso, só há uma forma de se proteger: criando uma sequência forte. Como? Veja abaixo:

8 caracteres ou mais: uma senha grande é mais difícil de ser descoberta;

Misture tudo: letras maiúsculas e minúsculas, números e símbolos;

Só pode ter números? Crie a ordem mais aleatória possível;

Não utilize dados pessoais (ex.: número de telefone) e nem palavras comuns (ex.: amor);

Não utilize sequências! Nem de letras, nem de números e nem códigos do teclado.

Está achando difícil?

Olha como é possível criar e memorizar uma senha forte e segura:

- Pense em uma frase que você gosta **(ex.: "O cravo brigou com a rosa")**;
- Anote a primeira letra de cada palavra da frase **(ex.: ocbcar)**;
- Acrescente algum símbolo e número **(ex.: ocbcar*28)**;
- Substitua algumas letras por números ou símbolos **(ex.: 0cbca!*28)**.

É possível ser seguro com **facilidade!**

Como cada conta precisa de uma senha própria, você pode usar gerenciadores ou cofres para armazenar com segurança suas senhas, sem ter a necessidade de memorizá-las. Ótimo, né? Algumas opções no mercado são o LastPass, True Key e 1Password.

Você também pode habilitar a **dupla autenticação** em aplicativos e dispositivos, aumentando o grau de proteção das suas informações. Essa segunda sequência não fica salva em base de dados. Caso seus dados sejam expostos, ainda é necessária essa informação para acessar a conta.

Repita esse processo com frequência

É bom **alterar sua senha** com certa regularidade (ex.: a cada 3 meses);

Quando comprar algum equipamento que venha com uma **senha padrão**, caso dos roteadores.

Em caso de **roubo ou furto** de celular, computador ou outro dispositivo;

Quando suspeitar que suas senhas ou contas foram **descobertas ou invadidas**;

3 Sua casa também é **segura?**

Nossas casas contam nossas histórias e, por isso, podem passar informações privadas para pessoas mal-intencionadas. Devemos prestar muita atenção nas maneiras como armazenamos e descartamos dados físicos e digitais.

Confira quais os hábitos você já possui e quais você precisa adquirir para ter uma rotina segura:

Você ainda recebe contas pelo **correio?**

Algumas pessoas são profissionais em procurar por informações no lixo. Achou que era coisa de filme? Não é!

Correspondências pessoais e que possuam dados sigilosos, como faturas de bancos e convênios médicos, também devem ser fragmentadas ao máximo. Jamais jogue esses documentos por inteiro no lixo.

Quebre todos os cartões, invalidando o chip antes de descartá-lo: cartão do banco, cartão fidelidade e todos os que possuírem dados sensíveis (como nome completo, data de nascimento, endereço e números de identificação).

Ligações e mensagens também devem ser **monitoradas**

Práticas como o ***Phishing*** e o ***Vishing*** são muito comuns no roubo de informações:

O Phishing é uma mensagem falsa, enviada por e-mail ou chat, que compartilha algum link ou arquivo malicioso para roubar informações e infectar equipamentos.

O Vishing é o trote telefônico que consegue tirar da pessoa dados sensíveis que podem ser utilizados para aplicar outros golpes.

Quando receber alguma mensagem que pareça suspeita, entre em contato com quem enviou a mensagem. Assim você pode confirmar se links e arquivos são seguros.

E lembre: não passe dados pessoais para desconhecidos, seja por mensagem ou ligação.

Não divida a internet com o vizinho

Se a rede é aberta, qualquer um pode acessá-la - inclusive invasores. Quando um mesmo sinal de wi-fi é compartilhado, fica mais fácil invadir equipamentos. Por isso, sempre que precisar usar a internet, prefira uma conexão própria, como seu 3G/4G ou rede particular.

Evite também utilizar as redes de wi-fi gratuitas disponíveis em locais públicos ou em ambientes como restaurantes e lojas.

O que é público pode ser usado **contra** você

As redes sociais são sites em que a navegação é livre. Qualquer um pode ter acesso ao seu perfil, independente das coisas que podem ser vistas. **Seu comportamento é seguro?**

- Adicione apenas quem você conhece e libere suas publicações apenas para seus amigos;
- Cuidado com bate-papo com desconhecidos, preste atenção ao que será dito;
- Não divulgue seus dados pessoais, seja nas publicações abertas, seja nas privadas;
- Evite informar sua localização, é possível rastrear comportamentos habituais;
- Cuidado para não mostrar demais em suas fotos. Imagens de dados bancários, por exemplo, podem acabar com um cartão clonado.

4 Como conversar com os **nativos** digitais?

Em 2014 a AVG (empresa de antivírus) realizou uma pesquisa com mães de crianças entre 0 e 4 anos, que chegou nos seguintes dados:

1/4 das crianças consegue acessar navegadores

19% conseguem usar aplicativos sozinhas

28% conseguem fazer ligações.

Crianças e adolescentes estão cada vez mais conectados e pais e responsáveis precisam estar atentos a todas as atividades de seus filhos na internet. Para isso é preciso ter conversas frequentes sobre bons comportamentos online.

O que seus filhos acessam na internet?

Redes sociais e games são as principais atividades de crianças e adolescentes na internet. Nesses ambientes, várias mensagens são trocadas, inclusive com pessoas que você - e elas - desconhece. O ideal é explicar para seus filhos que na internet nem todos são o que dizem ser, contar que existem golpes e ensinar como se proteger.

Algumas opções para você gerenciar o acesso dos seus filhos:

Deixe o dispositivo utilizado em um local compartilhado: assim você consegue ver as atividades realizadas;

Limite o tempo de navegação: estabeleça horários para entrar nas redes sociais;

Ative filtros de conteúdo: uma maneira de garantir que determinados termos não chegarão ao seu filho;

Crie listas negras no navegador: para evitar que sites específicos sejam acessados.

Seja um **exemplo** para a futura geração

Antes de cobrar um comportamento saudável de seus filhos, você também precisa ter hábitos seguros na internet. Converse com regularidade sobre comportamentos online:

Não repassar discursos de ódio;

Não repassar informações sem checar a fonte;

Não adicionar desconhecidos;

Não passar dados pessoais para desconhecidos.

E o que eles podem **ensinar** a você?

Jovens pegam as tendências com maior facilidade. Você pode aproveitar esse conhecimento em novas ferramentas e dispositivos para manter o diálogo com seus filhos a respeito de comportamentos online. Descobrir novos hábitos digitais tão logo eles surjam nos ajuda a perceber com antecedência novos golpes que podem ser criados.

5 É muito mais fácil comprar **online!**

O e-commerce está crescendo no Brasil. Em 2017 foram mais de R$47 bilhões em lucro e mais de 55 milhões de consumidores. Você pode comparar preços e produtos, receber o produto no dia seguinte, tudo sem sair da sua casa. Mas é preciso estar alerta para não entregar seus dados para pessoas mal-intencionadas.

Cuidado com golpes...

Muitos invasores aproveitam datas comemorativas e utilizam a identidade visual de marcas conhecidas para sequestrar dados. Lembre-se das dicas para evitar o Phishing!

Se receber mensagens de promoções,
procure nos canais oficiais da marca se é real;

Não clique em links suspeitos
(lembre-se das dicas de sites seguros);

Não forneça dados sensíveis,
como login, senha e números de documentos;

Não clique em pop-ups e banners suspeitos
e verifique se o site fez algum download automático.

Se escolher realizar a compra por algum aplicativo, faça o download pela loja oficial - como Apple Store ou Play Store. Um aplicativo falso também pode sequestrar informações do seu dispositivo, como os dados do seu cartão.

Escolha empresas com boas **recomendações**

Além das dicas para saber se o site é seguro, você também deve procurar dados da empresa na internet. O número do CNPJ e o endereço das empresas ficam disponíveis. Você pode entrar em contato para conferir essas informações.

Muitos sites e redes sociais também disponibilizam áreas para que outros consumidores deixem suas opiniões sobre o serviço prestado. Faça uma busca para saber se a empresa entrega o que promete antes de finalizar qualquer compra.

Escolha a forma de pagamento mais **segura**

Finalizar a compra é o momento mais sensível, porque é a hora em que você disponibiliza seus dados. Essas são as suas opções:

Cartão de débito/crédito: compras em lojas físicas ou virtuais passam pelo mesmo procedimento

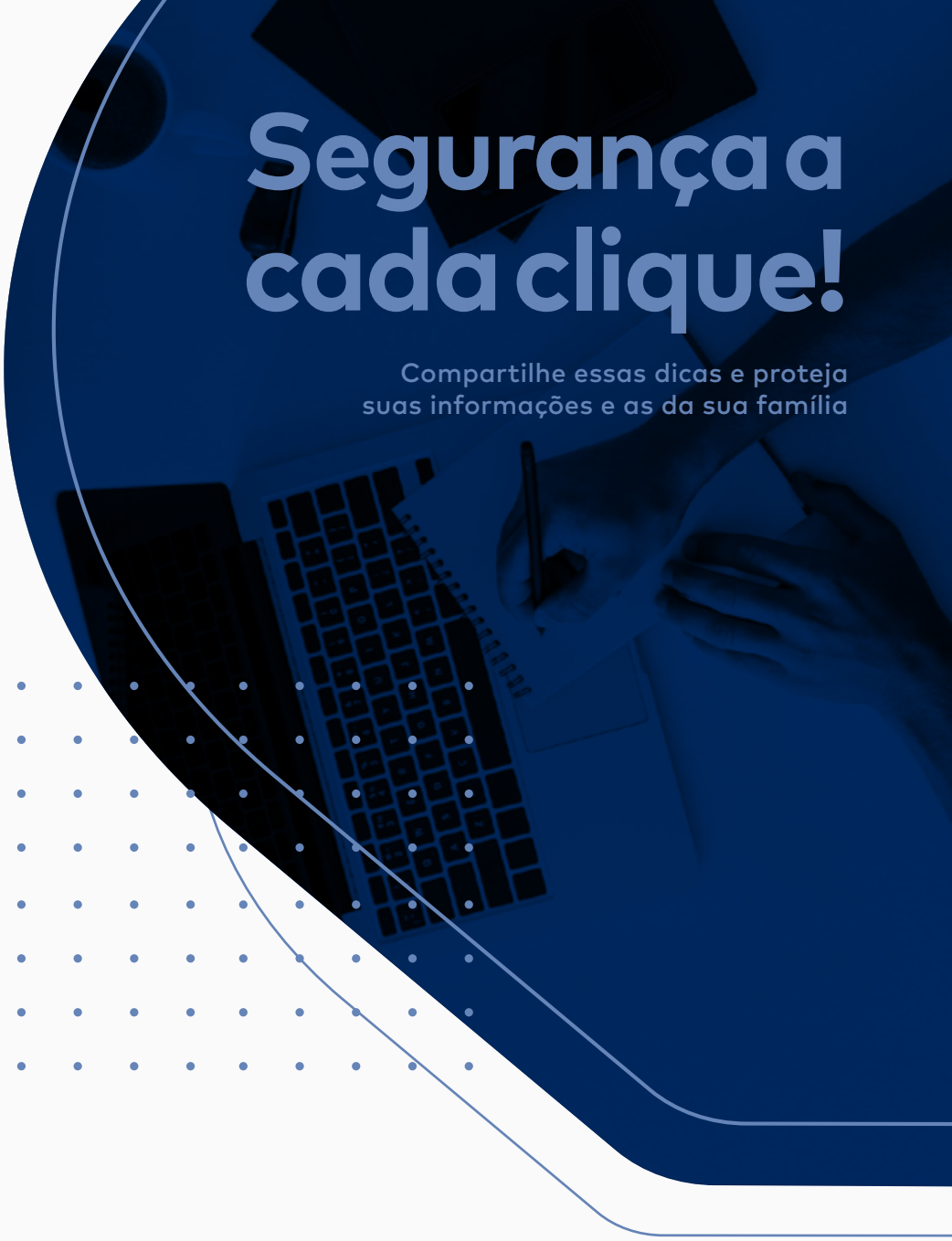
Pagamento on-line: serviços como o PayPal e o PagSeguro não compartilham informações pessoais do comprador com a loja;

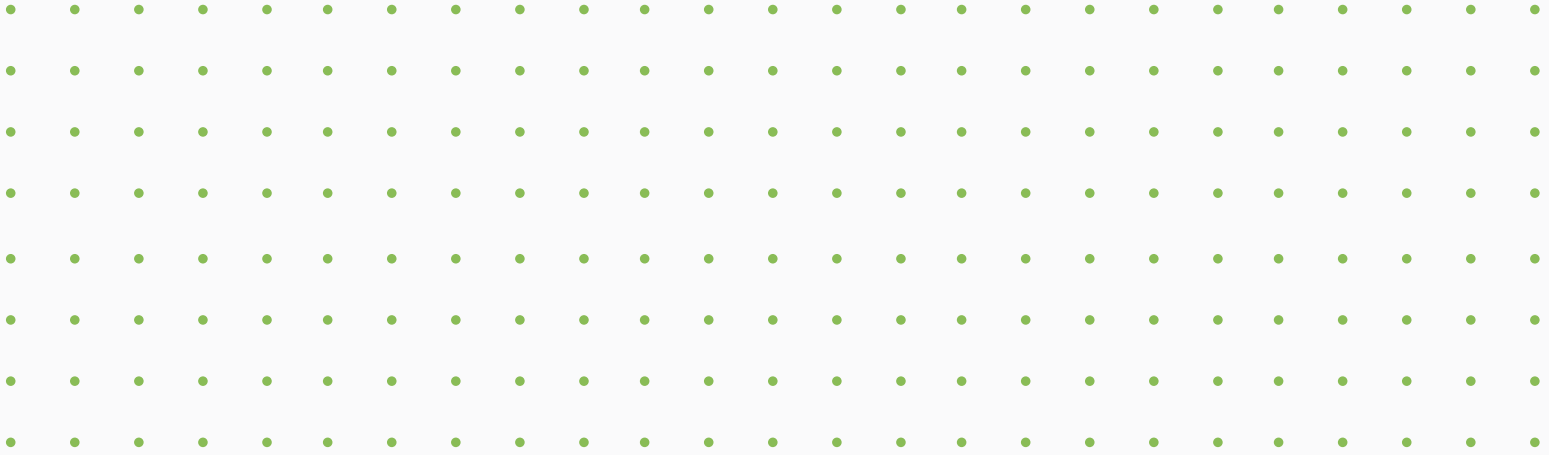
Boleto bancário: escolha a opção sem identificação, que permite que você não precise passar dados como número da conta e CPF.

É recomendado que todo o processo da compra online seja feito a partir de dispositivos próprios: seu computador ou seu celular.

Segurança a cada clique!

Compartilhe essas dicas e proteja suas informações e as da sua família





agibank®