

WHITEPAPER



SEGURANÇA DIGITAL PARA TERCEIRA IDADE



COMO DIMINUIR OS RISCOS
E NAVEGAR COM SEGURANÇA



gcsecurity

SEGURANÇA DIGITAL PARA TERCEIRA IDADE

COMO DIMINUIR OS RISCOS E NAVEGAR COM SEGURANÇA

É muito bom poder sentir-se mais próximo dos familiares e amigos, principalmente em tempos de isolamento social. Também é conveniente saber das notícias do mundo inteiro em tempo real, através do telefone celular ou de um computador. Pesquisar qualquer assunto que te interessa está ao alcance das mãos através da tecnologia. Tudo está conectado! Grandes empresas, pequenos negócios, familiares e amigos são todos digitais.

Mesmo sendo uma incrível fonte de informações, entretenimento, socialização e oportunidades, a **internet também oferece diversos riscos**. A internet é um espaço virtual público, gigante, que reúne todos os tipos de gente, assuntos e coisas. O universo digital depende de como as pessoas se comportam no espaço virtual: pode ser bom ou mau, perigoso ou seguro. Segurança cibernética também é sobre a redução de riscos pessoais. É muito difícil estar inteiramente seguro, não existe uma “bala de prata”, mas você pode se esforçar para se tornar um alvo mais difícil. Com mudanças rápidas e crescentes, é preciso adaptar-se constantemente às modernidades da era digital.



As redes sociais representam um meio de comunicação importante hoje, e nelas reunimos familiares, amigos, conhecidos, amigos virtuais e até desconhecidos. Assim como os golpes que acontecem em praças públicas, existem criminosos tentando aplicar golpes a todo momento na internet. Os casos são dos mais variados: **perfis falsos, de pessoas se passando por outras e tentando se aproximar para praticar fraudes, muitas vezes tiram proveito da fragilidade emocional da vítima**, para conseguir informações e dados pessoais. Existem até aqueles que se passam por boa-pinta e dizem-se apaixonados só para praticar crimes. Cuidado com o tal “amigo do amigo” nas redes sociais.

As armadilhas são das mais variadas. Existem websites criados somente para cometer fraudes e roubo de dados, se você se deparar com algo suspeito faça uma pesquisa sobre a empresa, verifique o CNPJ ou telefone para o número informado. **Cuidado com e-mails e mensagens de texto que parecem ser providas do seu banco, da polícia ou do governo.** Essas instituições não usam comunicação eletrônica para contatar, é muito provável que seja golpe, por isso nunca forneça suas informações pessoais ou dados bancários e não clique em links ou abra qualquer arquivo anexo. Entre em contato direto através de telefones oficiais para averiguar. E-mails de pessoas que você não conhece também devem ser tratados como suspeitos. É preciso ter cuidado e responsabilidade sempre, para desfrutar o melhor que o mundo digital tem a oferecer.

Para te ajudar a navegar com mais segurança e aproveitar o melhor da internet, listamos 10 dicas:

1. CRIE SENHAS FORTES

Muitos idosos não usam o recurso de senha nos seus dispositivos habilitados para internet, deixando-os mais vulneráveis. Bloqueie todos os seus dispositivos, incluindo computador, tablet e smartphone com senhas seguras. Isso adiciona uma linha de defesa caso você perca um de seus dispositivos ou em caso de roubo. **Uma senha forte deve conter pelo menos 12 caracteres intercalando letras, números e símbolos.** Sua senha é pessoal e intrasferível, não compartilhe com ninguém!



2. ACESSO SEGURO ÀS CONTAS

Senhas podem ser roubadas, adicionar autenticação em duas etapas às contas fornece uma camada adicional de proteção. Muitos aplicativos e sites oferecem essa opção que aumentam a proteção das suas informações e garantem que é você quem está acessando a conta. Pense que as configurações de segurança dos seus perfis nas redes são como **portões da sua residência: você tem de mantê-los fechados, trancados, para dificultar qualquer tentativa de invasão.**



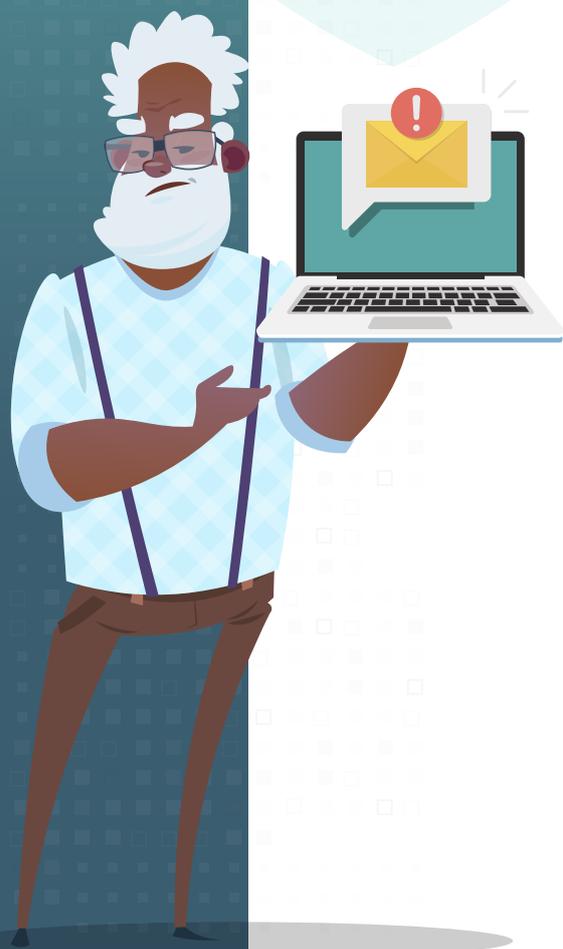
Autenticação em duas etapas é quando um segundo código é enviado para você todas as vezes que você acessa um site ou aplicativo.

3. PENSE DUAS VEZES ANTES DE CLICAR

E-mails e contatos que criam um **senso de urgência, como um problema em sua conta bancária ou com impostos, é muito provavelmente uma tentativa de golpe.** Considere entrar em contato diretamente com a organização em questão por telefone para determinar se o e-mail ou mensagem é legítimo ou não.

4. NA DÚVIDA, DELETE

Cliques errados permitem aos golpistas acessos a informações pessoais. **Se um e-mail ou mensagem parece duvidoso e incomum, mesmo que você conheça o remetente, é prudente excluí-lo.** Criminosos podem enviar e-mails com disfarce de pessoas conhecidas. Ative o filtro de spam da sua conta de e-mail para ajudar a conter mensagens suspeitas.



5. COMPARTILHE COM CUIDADO

Esteja ciente do que você compartilha publicamente nas mídias sociais. Ajuste suas configurações de privacidade para limitar quem pode ver suas informações. Evite compartilhar sua localização. No mundo virtual, temos a impressão de que ter muitos amigos nas redes é sinal de estar sempre feliz e de bem com a vida. Pense como se fossem pessoas andando na rua: não sabemos se são todas legais e bem-intencionadas. Conhecer pessoas através da internet pode ser muito divertido e interessante, mas não se deve confiar em estranhos. Muitas vezes, **a pessoa que está do outro lado da tela pode não ser quem pensamos ser**, por isso tome muito cuidado com as informações pessoais que você compartilha. Na internet, também podemos manifestar o que pensamos, através de fotos, vídeos e outros conteúdos. O mundo virtual também traz uma falsa sensação de anonimato, mas não se engane: quem faz comentários ou compartilha conteúdo que difame, caluniam e incitam preconceito ou outros crimes está sujeito às penas previstas em lei. O virtual é real e deixa rastros.

Eu te conheço da onde?



6. USE UM SOFTWARE DE SEGURANÇA

Instale um software de segurança em seus dispositivos e mantenha-o atualizado. É prudente executar o antivírus e anti-spyware com regularidade. Desconfie de atualizações de segurança que aparecem subitamente na tela ou em e-mails, elas podem ser malware e infectar seu computador ao invés de protegê-lo.

7. AJUSTE AS CONFIGURAÇÕES DE SEGURANÇA DO SEU NAVEGADOR

Você provavelmente procura por notícias, informações e produtos usando um navegador de internet como Firefox, Google Chrome, Internet Explorer e Safari. Ajuste suas **configurações em cada um desses navegadores para definir suas opções e melhorar a segurança**. Esses menus de configurações são geralmente encontrados no canto superior direito do seu navegador. Procure limpar seu histórico de navegação no final da sessão para que você não deixe um rastro de dados pessoais.



8. USE A PROTEÇÃO DE SEGURANÇA PADRÃO DO FIREWALL NO COMPUTADOR

O sistema operacional provavelmente tem **configurações padrão de firewall que protegem seu computador** sem precisar de ajuste. Se o seu software antivírus inclui proteção adicional de firewall que pode ser ajustado separadamente, considere entrar em contato com um profissional especializado para obter assistência e garantir que você esteja protegido sem bloquear os demais sites e programas que você usa regularmente.

9. NÃO SE ESQUEÇA DE FAZER LOGOUT

Lembre-se de **sair de aplicativos e sites quando terminar de usá-los**. Deixá-los abertos na tela do seu computador pode deixá-lo vulnerável a riscos de segurança e privacidade.

10. TENHA APOIO DE ALGUÉM

Se você vive sozinho, considere uma fonte confiável como um membro da família para te ajudar a ser mais vigilante. **Netos podem ter bastante experiência e disposição para ajudar**.



+55 (11) 2972-8999 

contato@gcsec.com.br 

São Paulo - SP 

Rua Jaceru, 384, conjunto 1907
Vila Gertrudes • 04705-000

www.gcsecurity.com.br 

Sobre a GC

Surgimos em 2008 e, desde então, trabalhamos incansavelmente para reduzir os riscos digitais em companhias de todos os setores e portes.

Ampliamos a visibilidade sobre vulnerabilidades e falhas de segurança para proteger ativos, dados, aplicações, usuários e sistemas.

Criamos um framework exclusivo que inclui práticas dos mais avançados padrões de segurança de mercado como NIST, PCI-DSS, ISO 27.001 e 27.005 e guiamos nossos clientes através da prevenção de riscos digitais, proteção e continuidade de negócios.

Pessoas

Nossa equipe é formada por mais de 20 profissionais especializados em segurança cibernética, com formação multidisciplinar, certificações técnicas e grande capacidade de pesquisa e desenvolvimento de proteções contra ameaças digitais.

A expertise em cyber security, gestão de vulnerabilidades, compliance, gestão de risco digital e ethical hacking permite que a gente crie soluções eficientes, sempre um passo à frente das táticas de ataque usadas por cibercriminosos.