

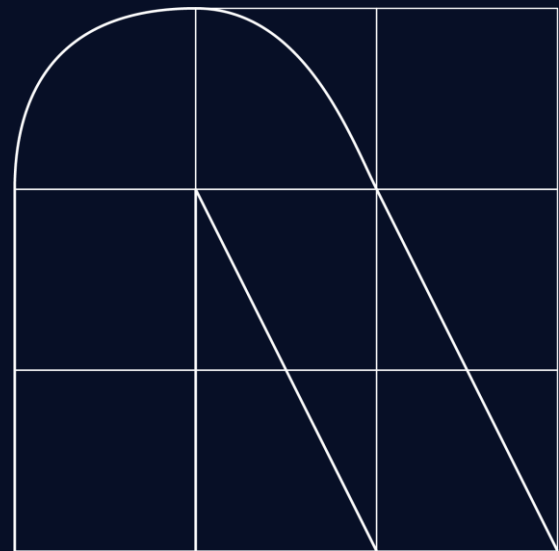


Outubro · Mês da Cibersegurança

Os 7 hábitos das pessoas altamente ciberseguras

Um guia breve para transformar boas decisões digitais em hábitos cotidianos.

A segurança começa em cada decisão.



A cibersegurança também é uma questão de hábitos

Pequenas decisões do dia a dia podem fazer uma grande diferença.

ANTES DE COMEÇAR

A segurança começa em cada decisão. Não é preciso ser especialista em cibersegurança para reduzir riscos. Muitas das decisões que protegem nossas informações, nossa identidade e nossa organização começam em ações simples que repetimos todos os dias.

As ameaças evoluem, as ferramentas mudam e a inteligência artificial torna algumas fraudes cada vez mais convincentes. Mas uma parte importante da segurança continua dependendo de decisões muito humanas: parar antes de clicar, verificar uma solicitação inesperada, proteger uma identidade ou avisar quando algo não parece certo.

Este guia reúne sete hábitos simples para colaboradores e cidadãos. O objetivo não é transformá-los em especialistas, mas ajudá-los a desenvolver um melhor senso crítico digital e a reagir com mais segurança a situações do dia a dia.

OS 7 HÁBITOS, EM UM RELANCE

- 01 Pense antes de clicar.
- 02 Proteja sua identidade digital.
- 03 Verifique antes de confiar.
- 04 Compartilhe apenas o necessário.
- 05 Mantenha seu ambiente digital atualizado.
- 06 Na dúvida, reporte
- 07 Aprimore seu senso crítico digital.



Controle o impulso. Proteja seu acesso

Dois hábitos básicos para reduzir riscos antes que se transformem em incidentes.

01

Pense antes de clicar

Muitas fraudes digitais buscam provocar uma reação imediata: urgência, medo, curiosidade ou a sensação de que precisamos agir antes de pensar. Um e-mail, uma mensagem ou um link pode parecer rotineiro e, justamente por isso, convincente.

O hábito mais útil é criar uma pequena pausa. Antes de abrir um arquivo, acessar um link ou responder a uma solicitação inesperada, observe o contexto: você esperava essa mensagem? O remetente é realmente quem diz ser? Está pedindo algo fora do comum? Alguns segundos de verificação podem evitar uma decisão difícil de reverter.



COLOQUE EM PRÁTICA

Pare por alguns segundos e verifique o remetente, o contexto e a solicitação antes de agir.

02

Proteja sua identidade digital

No ambiente digital, nossas credenciais representam quem somos e o que podemos fazer. Por isso, proteger uma conta não significa apenas escolher uma senha difícil: significa reduzir as chances de outra pessoa se passar por nós.

Use senhas diferentes para serviços distintos, ative a autenticação multifator sempre que estiver disponível e evite compartilhar códigos de acesso, mesmo quando a solicitação parecer vir de alguém conhecido. No trabalho, siga os procedimentos oficiais para solicitar ou conceder permissões. A identidade é uma porta de entrada; quanto melhor a protegemos, mais difícil é transformar uma credencial comprometida em um incidente maior.



COLOQUE EM PRÁTICA

Ative a MFA e não compartilhe senhas, códigos ou acessos por canais não oficiais.



Uma pausa na hora certa e uma identidade bem protegida são duas das decisões mais simples — e mais eficazes — que podemos transformar em hábitos.

Verifique. Compartilhe com critério.

A confiança digital se constrói verificando antes de agir e reduzindo a exposição desnecessária.

03

Verifique antes de confiar

A inteligência artificial pode fazer com que uma mensagem, uma voz ou uma imagem pareçam muito convincentes. Por isso, uma das competências digitais mais importantes é separar aparência de confiança: algo que “parece real” já não é suficiente para ser considerado autêntico.

Ao receber uma solicitação incomum relacionada a dinheiro, dados sensíveis, alterações de acesso ou informações confidenciais, confirme por um segundo canal. Uma ligação para um número que você já conhece, uma mensagem pelo canal corporativo ou uma verificação direta podem ser suficientes. Verificar não é desconfiar; é uma forma responsável de proteger as pessoas e a organização.



COLOQUE EM PRÁTICA

Para solicitações sensíveis ou incomuns, confirme sempre por um segundo canal confiável.

04

Compartilhe apenas o necessário

A segurança também depende do quanto expomos. Cada documento, dado, permissão ou conversa compartilhada aumenta o número de pessoas e sistemas que precisam proteger essas informações. Aplicar o princípio do “somente o necessário” reduz o risco sem complicar o trabalho.

Antes de enviar um arquivo, publicar informações ou conceder acesso, pergunte quem realmente precisa vê-las e por quanto tempo. Evite transferir dados sensíveis para canais não autorizados e confira os destinatários antes de clicar em “enviar”. Na vida pessoal, vale a mesma lógica: quanto mais publicamos sobre rotinas, viagens, trabalho ou relacionamentos, mais contexto oferecemos a quem tenta criar fraudes convincentes.



COLOQUE EM PRÁTICA

Revise destinatários, permissões e o canal antes de compartilhar informações ou arquivos.

Mantenha seu ambiente preparado e reporte rapidamente.

Atualizar e reportar são hábitos de prevenção e resposta, não tarefas exclusivamente técnicas.

05

Mantenha seu ambiente digital atualizado

Atualizar não significa apenas incorporar novas funcionalidades. As atualizações corrigem erros e vulnerabilidades que podem ser explorados por cibercriminosos. Adiá-las indefinidamente pode deixar aberta uma porta que já sabemos como fechar.

Transforme a atualização em rotina: instale atualizações de sistemas e aplicativos quando necessário, reinicie os dispositivos quando solicitado e evite instalar software de fontes não confiáveis. Em ambientes corporativos, respeite as políticas de atualização da organização e não tente desativar controles apenas porque são incômodos. Um ambiente digital bem cuidado é menos vulnerável e mais fácil de proteger.



COLOQUE EM PRÁTICA

Atualize quando necessário e use somente softwares e canais autorizados.

06

Na dúvida, reporte

Uma mensagem suspeita, um acesso estranho ou até mesmo um clique acidental não devem ser escondidos. Quanto antes uma organização souber de um possível incidente, mais opções terá para analisá-lo, contê-lo e reduzir seu impacto.

Reportar não significa ter certeza de que existe um ataque. Significa compartilhar um sinal para que ele possa ser avaliado. Se você abriu um arquivo suspeito, digitou uma senha onde não deveria ou percebeu um comportamento estranho, use o canal definido pela sua organização o mais rápido possível. Na vida pessoal, altere as credenciais quando necessário e entre em contato com o serviço afetado pelos canais oficiais.



COLOQUE EM PRÁTICA

Se algo não parecer certo, reporte rapidamente. Um alerta antecipado pode reduzir o impacto.

Aprimore seu senso crítico digital

A cultura de segurança se constrói quando o aprendizado deixa de ser pontual e se torna uma prática contínua.



07

Aprimore continuamente seu senso crítico digital

As ameaças mudam porque a tecnologia, os canais e nossos próprios hábitos também mudam. Um treinamento realizado uma vez por ano pode ajudar, mas a verdadeira cultura de segurança se constrói quando aprendemos de forma contínua e aplicamos esse aprendizado a situações reais.

Participe dos treinamentos, simulações e comunicações de segurança disponíveis. Preste atenção a novos tipos de fraude e compartilhe aprendizados com colegas, familiares ou pessoas com menos experiência digital. O objetivo não é viver em alerta permanente, mas reconhecer padrões, fazer perguntas melhores e saber o que fazer quando surgir uma situação inesperada.



COLOQUE EM PRÁTICA

Revise seus hábitos periodicamente e compartilhe o que aprendeu com as pessoas ao seu redor.



SETE HÁBITOS. UMA MESMA IDEIA.

Não é preciso ser especialista em cibersegurança para tomar melhores decisões de segurança. É preciso transformá-las em hábitos: parar, verificar, proteger, compartilhar com critério, atualizar, reportar e continuar aprendendo.

A segurança começa em cada decisão

Saiba como a NTT DATA pode ajudar sua organização a fortalecer a cultura de segurança por meio de treinamento contínuo e experiências de aprendizagem adaptadas às suas necessidades.



Entre em contato com grupo.hacking@nttdata.com para obter informações sobre Treinamento e Conscientização em Cibersegurança

