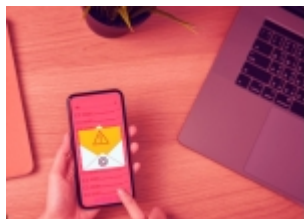


SEMPRE ALERTA: Serasa dá dicas para aumentar segurança digital e fugir de golpes na internet



Em meio ao aumento de fraudes no ambiente digital, proteger informações pessoais e entender os riscos da internet tornou-se essencial. Para ajudar os brasileiros nessa missão, a Serasa relança a série Sempre Alerta, que traz conteúdos educativos sobre segurança digital. No primeiro conteúdo desta nova temporada, Eduardo Cachola, gerente da Carteira de Dados Serasa, traz cinco dicas práticas para redobrar os cuidados com dados pessoais e financeiros.

“A segurança digital está presente em vários momentos do dia a dia, desde quando o consumidor acessa um aplicativo bancário, faz uma compra online, entra nas redes sociais ou preenche um formulário com seu CPF”, explica Eduardo. “A internet é um espaço público e, assim como trancamos a porta de casa, também precisamos fechar os caminhos para golpes e proteger a vida online”.

Prejuízos financeiros

Mesmo com a grande propagação de golpes, ainda é comum que usuários mantenham hábitos pouco seguros, como senhas fracas, desabilitação da autenticação de dois fatores, Face ID e entre outros. De acordo com dados da Kaspersky, empresa especializada em cibersegurança, 58% dos brasileiros não trocam suas senhas com frequência. Além disso, levantamentos apontam que a senha mais usada no país ainda é "123456".

Segundo Eduardo, as ameaças também evoluíram, e novas formas de ataques surgem diariamente. "Atualmente, muitos golpes nem precisam da senha diretamente. O criminoso finge ser um conhecido ou representante de alguma empresa para convencer a vítima a fornecer códigos de acesso, cliques em links ou outras informações", explica. "Mesmo a melhor senha pode ser comprometida. Por isso, adotar outras camadas de proteção online é indispensável”.

O especialista ainda reforça que a atuação dos golpistas também pode causar prejuízos financeiros significativos para as vítimas. “Além dos danos psicológicos, esses tipos de fraudes também impactam diretamente no bolso das famílias, já que os criminosos se aproveitam da situação já vulnerável dos consumidores. Por isso, alertar e orientar para boas práticas no ambiente digital é também uma forma de apoiar uma jornada financeira completa e ainda mais segura”, afirma.

Como reforçar a segurança digital?

Para ampliar os níveis de precaução no ambiente online, Eduardo Cachola reúne cinco dicas para

ajudar os brasileiros de forma prática:

Crie senhas fortes

Uma senha forte é aquela que é composta por, pelo menos, 12 caracteres, misturando letras maiúsculas e minúsculas, números e símbolos (como !, #, @). Ao criar senhas, evite usar informações pessoais, como data de nascimento, nome ou sequências simples. Quanto mais imprevisível, melhor. Também é muito importante que as senhas sejam únicas — não sejam usadas em mais de um serviço ou plataforma.

"Senhas únicas fracas ou repetidas podem ser portas de entrada para um efeito dominó de invasões", alerta o especialista. "Uma dica extra é utilizar gerenciadores de senhas confiáveis para gerar combinações ainda mais seguras, atrelando também à possibilidade de armazená-las com criptografia,".

Ative a autenticação em dois fatores

A autenticação exige uma segunda etapa de verificação, que pode ser feita via SMS, app autenticador, token ou até mesmo por uma confirmação via e-mail. Ao prosseguir com a autenticação de dois fatores, mesmo que sua senha entre em contato com outras pessoas, invasor será impedido de entrar, pois precisará desse código ou token para finalizar o acesso.

Utilize biometria, reconhecimento facial e tokens

O uso da biometria, seja ela digital ou facial garante que só você consiga acessar determinados serviços. Tokens físicos ou digitais também aumentam a segurança de transações financeiras. "Atualmente, muitos bancos e instituições financeiras já utilizam desse recurso para proteção. Em alguns celulares, também já é possível habilitar essa camada de proteção", comenta Eduardo.

Adote uma identidade digital verificada

Essa nova camada de proteção segura e armazena as credenciais com criptografia e autenticação avançada, reduzindo a necessidade de criar logins em cada site e permitindo validar o acesso em poucos cliques — com segurança e consentimento.

"Essa identidade funciona como um RG digital. A verificação é feita de forma online por uma plataforma confiável que checa suas informações e confirmam a autenticidade", detalha.

Cuidado com links e redes suspeitas

Links maliciosos são uma das formas mais comuns de aplicar golpes. "Desconfie de mensagens com endereços que prometem ofertas, prêmios ou alertas muito descolados da realidade, que se utilizam desse senso de urgência como gatilho para se aproveitar dos consumidores mais desavisados", indica Eduardo. A orientação é de checar o remetente de e-mails ou mensagens nas

redes sociais e buscar por selos de verificação. Caso tenha dúvidas, não clique no link, nem preencha formulários com seus dados. Acesse sempre os canais oficiais, digitando o endereço direto no navegador ou diretamente pelo aplicativo próprio.

Além disso, o especialista também destaca os cuidados ao se conectar em redes Wi-Fi públicas, como em cafés, aeroportos ou shoppings. “Essas conexões podem ser vulneráveis. O ideal é usar uma VPN, que cria um túnel criptografado para proteger sua navegação”, conclui.

Eduardo ainda reforça a importância da educação financeira para garantir a segurança dentro e fora das redes: “A maior parte dos golpes se apoia em pressão, urgência ou confiança excessiva. Ao entendermos como eles funcionam e evitarmos cliques errados, já eliminamos boa parte do risco”.

Foto: Divulgação

<https://www.jornalpanfletus.com.br/cp3.masterix.inf.br/noticia/7006/sempre-alerta-serasa-da-dicas-para-aumentar-seguranca-digital-e-fugir-de-golpes-na-internet-em-30/06/2026-06:04>