Fascículos da Cartilha de Segurança para Internet trazem orientações sobre como resguardar informações pessoais, financeiras e senhas no ambiente online, e o que fazer em caso de vazamento

Publicações democratizam conhecimento sobre proteção de dados pessoais (Imagem: Divulgação/NIC.br).

Por ocasião do Dia Internacional da Proteção de Dados, celebrado globalmente em 28 de janeiro, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) lança dois novos fascículos da Cartilha de Segurança para Internet, cujos temas são “Proteção de Dados” e “Vazamento de Dados”. As publicações, que contam com contribuição da Autoridade Nacional de Proteção de Dados (ANPD), têm como objetivo conscientizar sobre a importância da proteção de dados e segurança da informação.

No fascículo “Proteção de Dados” o leitor vai aprender como adotar uma postura preventiva e diminuir a exposição de informações sobre si na Internet, além de como usar ferramentas de segurança e como se apoiar na legislação em caso de necessidade. “Uma novidade foi a adição das definições de alguns termos usados na LGPD, para facilitar o entendimento das políticas de privacidade e proteção de dados que o cidadão poderá encontrar em sites, serviços e aplicativos. É importante que cada pessoa conheça seus direitos e saiba a quem recorrer”, afirma Cristine Hoepers, gerente do CERT.br/NIC.br.

“Acreditamos que a informação é fundamental para que os titulares de dados exerçam os seus direitos. Por meio da disseminação do conhecimento, também reforçamos o nosso compromisso com o fortalecimento de uma cultura de proteção de dados pessoais do País”, declarou o Diretor-Presidente da ANPD, Waldemar Gonçalves.

Complementar ao primeiro material, o fascículo “Vazamento de Dados” traz orientações sobre como reduzir o impacto do acesso indevido, da coleta e da divulgação de informações pessoais na Internet. “Com o aumento de serviços online, os dados dos usuários ficaram mais expostos, o que torna mais comuns os vazamentos. No material, mostramos o que fazer quando um vazamento acontece - as ações diferem dependendo das informações afetadas, se são financeiras, senhas ou relacionadas à identidade”, adianta Cristine.

Cristine Hoepers complementa indicando que “dados são ativos valiosos e precisamos cuidar deles com o maior zelo possível. Se forem vazados, é fundamental agir rapidamente para diminuir o impacto dos danos. Ambos os fascículos contêm instruções importantes sobre o assunto”.

Os fascículos podem ser acessados gratuitamente. Para conhecer as publicações “Proteção de Dados” e “Vazamento de Dados” na íntegra, clique, respectivamente, aqui e aqui.

Confira abaixo algumas orientações do Fascículo “Proteção de Dados”:

Reduza dados sobre você na Internet – o excesso de exposição online pode comprometer sua privacidade e dar a golpistas a oportunidade de usar seus dados para, por exemplo, tentar se passar por você. Por isso, pense bem antes de postar algo. Ao fazer cadastros em sites e aplicativos, só forneça dados que sejam obrigatórios; seja seletivo ao aceitar seus contatos, pois quanto maior sua rede, mais pessoas terão acesso a seus dados. Também respeite os dados das outras pessoas.

Reduza a coleta de dados por sites – os sites que você acessa podem coletar dados de seu navegador, usá-los para traçar seu perfil comportamental e, com base nele, oferecer conteúdos personalizados para influenciá-lo, ou limitar suas opções. É importante que você avalie e ajuste as

configurações de privacidade de seu navegador; limite a coleta de dados por cookies e limpe com frequência o histórico de navegação – se possível, use navegação anônima.

Cuidado com perfis falsos – para ter acesso a seus dados, golpistas podem criar perfis falsos em redes sociais, tentando se passar por pessoas ou empresas conhecidas. Antes de aceitar como contato ou seguir alguém nas redes sociais, tenha certeza de que o perfil é legítimo e busque pelo selo indicativo de conta verificada. Se, ao receber um pedido de conexão, você ficar na dúvida, busque o perfil oficial da pessoa ou empresa, e bloqueie e denuncie perfis falsos.

Veja agora dicas do fascículo “Vazamento de Dados”:

Soube de vazamento de dados que pode afetá-lo? O que fazer? – Se receber de uma empresa um comunicado de vazamento de dados, ou souber por terceiros de algum vazamento que potencialmente o afete, é importante confirmar a veracidade e atuar prontamente para minimizar o impacto. É preciso ainda ficar alerta contra possíveis golpes. Para isso, confirme a veracidade via canais oficiais; procure entender quais dados vazaram, quando ocorreu o vazamento, quais as medidas de mitigação adotadas pela empresa e as execute.

Troque imediatamente senhas expostas – senhas vazadas podem levar a golpes contra você e seus contatos. Um atacante pode explorar recursos de recuperação de senhas para invadir outras contas suas (como de instituições financeiras) ou se passar por você e aplicar golpes em seus contatos. Troque a senha vazada em todos os serviços onde é usada (não repita senhas!); siga os procedimentos para recuperação da conta, caso ela tenha sido invadida e você não consiga acesso. Ative a verificação em duas etapas, se ainda não tiver feito, e analise registros de acesso e denuncie acessos indevidos.

Informe instituições financeiras – dados bancários e de cartões de crédito, se vazados, podem ser usados em fraudes ou para obtenção de empréstimos em seu nome. Por isso, é fundamental informar o vazamento às instituições envolvidas. Revise os extratos de cartões e contas bancárias, conteste lançamentos irregulares via canais oficiais e bloqueie ou substitua os cartões.

Fique alerta contra golpes – após um vazamento, é esperado um aumento nas tentativas de golpes por diferentes meios, como mensagens de texto, e-mails e ligações telefônicas. Podem ocorrer desde phishing direcionado até tentativas de extorsão para não expor seus dados. Para evitar transtornos, não clique em links recebidos por e-mail ou mensagens de texto, mesmo que pareçam convincentes; antes de efetivar transações financeiras, confirme os dados do destinatário (um golpista pode estar se passando por outra pessoa) e denuncie se criarem perfil falso em seu nome – não se esqueça de informar seus contatos, para que não caiam em golpes.

Cidadão na Rede

Para reforçar a mensagem, o NIC.br também lançou dois vídeos do Cidadão na Rede sobre os temas dos fascículos, “Proteção de Dados” e “Vazamentos de Dados”. Ambos podem ser acessados por meio do link: https://cidadaonarede.nic.br/ . Em animações de 15 segundos, o projeto difunde e incentiva boas práticas relacionadas à cidadania digital e ao bom uso da Internet.

Você também pode conferir e baixar gratuitamente em https://cidadaonarede.nic.br/ os mais de 100 vídeos disponíveis.

Sobre o CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Sua missão é aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no País. Para atingir esse objetivo, além de atividades de tratamento a incidentes, o Centro também investe na conscientização sobre os problemas de segurança, no auxílio ao estabelecimento de novos CSIRTs no Brasil e no aumento da

consciência situacional sobre ameaças na Internet, sempre respaldados por uma forte integração estabelecida com as comunidades nacional e internacional de CSIRTs. Mais informações em https://cert.br/.

Sobre o Ceptro.br

O Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações do NIC.br – Ceptro.br (https://ceptro.br/) tem por objetivo desenvolver projetos que visem a melhoria da qualidade da Internet e disseminar o seu uso, com especial atenção para seus aspectos técnicos e de infraestrutura. Para tanto faz medições, análise e projetos para melhorar a qualidade da Internet no Brasil, estimulando seu uso responsável e incentivando a adoção de boas práticas operacionais e de tecnologias relevantes. As ações em curso envolvem: o Portal Medições (https://medicoes.nic.br/), que reúne soluções para verificação da qualidade da Internet para consumidores, provedores e órgãos públicos, realizadas por meio do Sistema de Medição de Tráfego (SIMET); a disponibilização de servidores de tempo (NTP.br) que permitem a sincronização gratuita e segura com a Hora Legal Brasileira; o compartilhamento de caches de CDNs com o OpenCDN (https://opencdn.nic.br), possibilitando uma distribuição mais estruturada do conteúdo na Internet; cursos, eventos e outras atividades (https://ceptro.br/cursos-eventos), contribuindo para a capacitação da comunidade técnica da Internet e para a adoção de tecnologias importantes como IPv6 e RPKI; criação e disseminação de conteúdo com o Cidadão na Rede (https://cidadaonarede.nic.br), oferecendo orientações práticas para o melhor uso da Internet, no formato de vídeos curtos; entre outras atividades.

Sobre o Núcleo de Informação e Coordenação do Ponto BR – NIC.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (https://nic.br/) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. O NIC.br implementa as decisões e projetos do Comitê Gestor da Internet no Brasil - CGI.br desde 2005, e todos os recursos arrecadados provêm de suas atividades que são de natureza eminentemente privada. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil. Do NIC.br fazem parte: Registro.br (https://registro.br/), CERT.br (https://cert.br/), Ceptro.br (https://ceptro.br/), Cetic.br (https://cetic.br/), IX.br (https://ix.br/) e Ceweb.br (https://ceweb.br/), além de projetos como Internetsegura.br (https://internetsegura.br/) e Portal de Boas Práticas para Internet no Brasil (https://bcp.nic.br/). Abriga ainda o escritório do W3C Chapter São Paulo (https://w3c.br/).

Sobre o Comitê Gestor da Internet no Brasil – CGI.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (https://cgi.br/resolucoes/documento/2009/003). Mais informações em https://cgi.br/.

Com informações do NIC.br

Fonte: ANPD, em 23.01.2024.