BIM
Boletim Informativo Mensal
Comunicar para Educar
Dezembro/2022 – Ano 3 – nº 34

CUIDADOS COM COMPRAS NA *INTERNET*

Na hora de realizar compras na *internet*, é preciso estar atento para não se tornar vítima de um golpe virtual. Muitos criminosos utilizam métodos para enganar e obter vantagens financeiras sobre os consumidores. É importante que todos saibam dos riscos e conheçam as boas práticas em segurança cibernética.

Alguns passos nos ajudam a evitar certos tipos de golpes na internet. Detalhamos, abaixo, alguns deles.

• Valor de mercado do produto

– Desconfie de valores muito abaixo do praticado no mercado ou com grandes descontos.

– Verifique o histórico de preço em *sites* de busca e de comparação de valores de produtos e certifique-se de que o valor cobrado está condizente com a realidade

• Lojas *on-line*

– Procure comprar sempre em lojas conhecidas pelo grande público.

– Verifique a reputação da loja ou do vendedor onde o produto foi anunciado, em *sites* de reclamação e na área de comentários, se disponível.

– Observe se a página da loja possui o certificado de SSL, um pequeno cadeado do lado esquerdo da URL. É mais uma garantia de confiabilidade.

• Serviço de Atendimento ao Consumidor (SAC)

– Verifique a existência desse serviço onde deseja realizar suas compras. Grandes lojas possuem serviço dedicado à resolução de problemas sobre pagamentos, fraudes e entrega de produtos.

• *Phishing*

– Evite clicar em mensagens de *e-mail*, SMS ou de redes sociais que contenham *links* para *sites* com promoções. Alguns *links* podem levar para endereços falsos e maliciosos que solicitam dados pessoais e número de cartão de crédito.

– Digite diretamente na barra de endereços do navegador o endereço da loja que enviou o *e-mail* e localize a promoção indicada. Se desconfiar da mensagem recebida, descarte-a imediatamente.

• Formas de pagamento

– Gere o boleto diretamente no *site* da loja, verifique o código de barras e o nome do beneficiário. A situação não é diferente quando o pagamento for realizado por meio de PIX. Antes de confirmar o pagamento, verifique a chave e o nome do destinatário.

– Para pagamentos com cartão de crédito, se possível, utilize a modalidade de cartão virtual do seu banco ou operadora de cartão. Pois é um tipo de cartão que tem a possibilidade de expirar em poucos dias, não sendo permitida sua utilização após a sua data de validade. E caso o site sofra um ataque cibernético e tenha os dados dos consumidores vazados, o cartão virtual poderá ser desabilitado sem a necessidade de cancelamento do cartão físico.

• Computadores públicos

– Não utilize computadores públicos para realizar compras *on-line*. Computadores em redes e/ou compartilhados por diversas pessoas, como em *lan houses*, hotéis, escolas e universidades, podem conter *malwares* que roubam dados pessoais ao serem inseridos nos *sites* de compras. Utilize sempre seu próprio computador ou *smartphone* para realizar atividades que envolvam a transmissão de informações pessoais e bancárias.

– Instale um *software* antivírus confiável e mantenha-o sempre atualizado.

Com estas dicas é possível reduzir os riscos e aproveitar com mais segurança as promoções da *internet*.

O que é Gestão de Segurança da Informação?

A Gestão de Segurança da Informação não se limita à tecnologia da informação, é o processo que visa integrar às ações institucionais estratégicas, operacionais e táticas, as atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional.

Conforme a Instrução Normativa nº 03 do Gabinete de Segurança Institucional da Presidência da República (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172), sobre a qual já escrevemos em edições anteriores, observa-se que **a gestão de segurança da informação deve ser mantida e implementada de forma contínua**, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar o alcance dos objetivos do órgão ou da entidade.

Devido à importância da Gestão de Segurança da Informação, o Departamento de Segurança da Informação (DSI) tem uma Coordenação-Geral para tratar do tema, a Coordenação-Geral de Gestão de Segurança da Informação (CGGSI).

Entre as atribuições desse setor, destacamos:

- elaborar propostas de diretrizes, estratégias, recomendações e normas, incluindo decretos e projetos de lei;
- acompanhar a execução das ações da Política e do Plano Nacional de Segurança da Informação, bem como da Estratégia Nacional de Segurança Cibernética (E-Ciber);
- acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica;
- elaborar pareceres técnicos acerca de Projetos de Lei e outras proposições legislativas sobre segurança cibernética e da informação, em trâmite no Congresso Nacional;
- planejar, elaborar, estudar e participar de negociações de atos internacionais de caráter geral; e
- representar o GSI em diversos organismos internacionais.

Você sabia?

Os responsáveis pelo recebimento do documento com informação classificada em qualquer grau de sigilo, independente do meio e formato, devem:

- registrar o recebimento do documento;
- verificar a integridade do meio de recebimento, e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e
- informar ao remetente o recebimento da informação, no prazo mais curto possível.

Além disso, para os casos em que a tramitação de informação classificada ocorra por expediente ou correspondência, o envelope interno somente poderá ser aberto pelo destinatário, seu representante autorizado, ou autoridade hierarquicamente superior.

Mas, se o envelope interno estiver com a marca “PESSOAL”, somente poderá ser aberto pelo próprio destinatário.

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br