Cuidado com ofertas imperdíveis

A internet se tornou uma aliada essencial nas atividades diárias, oferecendo conveniência, rapidez e praticidade em diversas tarefas. Contudo, a facilidade de acesso a uma infinidade de informações e ofertas abre portas para fraudes e golpes, especialmente quando disfarçadas de ofertas imperdíveis.

Ofertas irresistíveis e descontos enormes podem parecer tentadores, mas é preciso ter cuidado: essas promoções são iscas frequentemente usadas por cibercriminosos para atrair vítimas e obter informações pessoais ou financeiras. Por isso, é fundamental adotar uma postura crítica e investigativa diante dessas situações para proteger seu dinheiro e sua segurança online.

Desconfie de ofertas boas demais para serem verdade

Quando uma oferta parece boa demais para ser verdade, há grande possibilidade de fraude. Golpistas utilizam a promessa de grandes descontos para induzir as pessoas a tomar decisões precipitadas, como clicar em links suspeitos, fornecer dados pessoais ou realizar pagamentos em páginas falsas. Antes de se deixar levar pela tentação, reserve um momento para avaliar a autenticidade da oferta. Nunca tome decisões precipitadas.

Como identificar ofertas suspeitas:

- ✓ **Pesquise sobre a oferta:** antes de fazer qualquer compra, verifique informações sobre o site ou vendedor. Verifique também avaliações de outros clientes em sites externos.
- ✓ **Desconfie de preços abaixo do mercado:** se o preço estiver significantemente abaixo do valor médio praticado, isso pode ser um indício de fraude ou erro. Compare com outros sites e desconfie de descontos exagerados.
- ✓ **Urgência na compra:** ofertas que pressionam para uma compra imediata, alegando limitação de estoque ou tempo limitado muito curto, podem ser golpes. Criminosos utilizam essa tática para evitar que a vítima tenha tempo de investigar.
- ✓ **Ofertas por tráfego pago:** desconfie de e-mails ou anúncios no Instagram que venham de contas não verificadas. Empresas confiáveis costumam enviar os anúncios através de e-mails corporativos reais e contas verificadas.

Proteja seus documentos e formulários

A proteção de documentos e formulários contendo informações pessoais e financeiras é essencial. Embora sejam comuns e parte da rotina, muitas vezes as pessoas subestimam a importância de proteger esses documentos de acessos indevidos.

Criminosos podem utilizar as informações contidas nesses documentos para cometer fraudes, como roubo de identidade, abertura de contas fraudulentas e até mesmo realizar compras ou contrair dívidas no nome da vítima. Por isso, é fundamental adotar práticas de segurança para proteger suas informações.

Por que proteger seus documentos?

Documentos que contêm informações pessoais, como nome completo, CPF, endereço e dados bancários, podem ser usados por criminosos para atividades ilícitas, o que pode resultar em prejuízos financeiros e complicações legais. A exposição desses dados pode facilitar a criação de contas fraudulentas ou transações indevidas, colocando em risco sua segurança pessoal, legal e financeira.

Como proteger seus documentos:

- ✓ **Evite imprimir desnecessariamente:** sempre que possível, prefira armazenar documentos de forma digital, com proteção por senha ou criptografia. Quando for necessário acessá-los, utilize plataformas seguras e confiáveis.

- ✓ **Não compartilhe documentos pessoais na internet:** evite enviar cópias de documentos em sites ou aplicativos que não sejam de confiança. Plataformas não verificadas podem expor seus dados a terceiros.

- ✓ **Cuidado com pedidos suspeitos:** antes de compartilhar qualquer documento, certifique-se de que a solicitação é legítima. Não forneça informações pessoais sem uma necessidade clara e somente durante o fechamento de contratos ou transações oficiais.

Ligações telefônicas suspeitas

As ligações de bancos são comuns no dia a dia, oferecendo serviços financeiros ou sugestões para sua conta. No entanto, é preciso estar atento: criminosos têm se aproveitado dessa prática para aplicar golpes, se passando por atendimento de bancos. Essas ligações buscam se passar por atendentes e informar supostas transações ou compras não reconhecidas.

Além disso, golpistas também oferecem propostas de investimento imperdíveis, muitas vezes associadas a utilização da margem consignável ou um suposto investimento em empréstimos para terceiros.

Assim, golpistas utilizam técnicas sofisticadas para parecerem confiáveis e tentam induzir ao fornecimento de informações, como senhas e dados pessoais, bem como ao envio de dinheiro ou assinatura de contratos fraudulentos.

Como identificar ligações suspeitas:

- ✓ **Desconfie de alertas de compra: s**empre verifique as compras e transações suspeitas no aplicativo do banco. Não confie nas informações vindas apenas pelo telefone.

- ✓ **Não forneça sua margem consignável:** evite promessas que queiram utilizar sua margem consignável em troca de rendimentos altos.

- ✓ **Evite decisões rápidas:** evite aceitar propostas que exigem resposta imediata e urgente. Financeiras legítimas permitem que você analise as condições com calma;

- ✓ **Não faça pagamentos adiantados:** um dos sinais mais frequentes de golpe é quando solicitam pagamento adiantado de eventuais "taxa de segurança" ou outros valores. Instituições legítimas nunca solicitam pagamento adiantado para conceder empréstimos ou outras condições especiais.

Proteja seu cartão de crédito

O cartão de crédito é uma ferramenta financeira poderosa e prática, permitindo que façamos compras com facilidade, seja online ou em lojas físicas. No entanto, seu uso indiscriminado e sem as devidas precauções pode abrir portas para fraudes, clonagem, compras não autorizadas e roubo de identidade. Garantir a segurança do cartão é essencial para proteger seu dinheiro e tranquilidade.

Com a evolução dos cartões, é possível pagar por aproximação, gerar cartões virtuais e limitar compras por cartão. Nesse contexto, golpistas se modernizam e utilizam diversas táticas para obter dados do cartão, seja através de ataques virtuais ou abordagens diretas. Assim, é importante utilizar as mais diversas ferramentas disponíveis para evitar se tornar uma vítima.

Como proteger seu cartão de crédito:

- ✓ **Cuidado com aproximação:** O pagamento por aproximação aprimora a segurança por não exigir a entrega do plástico. Porém, é importante sempre verificar o valor na tela da máquina e evitar deixar em bolsos traseiros ou expostos, evitando seu uso indesejado pela aproximação.

- ✓ **Uso de cartão virtual:** Evite o uso do cartão físico em compras online. É possível, na maioria dos aplicativos dos bancos, a emissão de cartão virtual para efetuar compras. Com eles, é possível definir uma utilização específica e não expor o número do principal, podendo limitar valores, quantidade de usos e validade.

- ✓ **Monitore suas transações:** É importante monitorar todas as transações no cartão, reportando ao banco emissor as compras indevidas que eventualmente ocorram o quanto antes.

Mantenha sua conta segura

A segurança bancária hoje é mais importante do que nunca. Com o aumento das transações digitais e o uso de dispositivos móveis, proteger a conta contra fraude e acessos indevidos é uma prioridade. Pequenas medidas de segurança podem fazer uma grande diferença na proteção do seu dinheiro e das informações pessoas.

Golpistas e hackers estão sempre à espreita, buscando brechas para acessar contas e realizar transações indevidas. Os ataques cibernéticos sempre tem seu alvo preferencial o elo mais fraco. Assim, é importante adotar práticas para aumentar a segurança das suas contas bancárias e garantir a segurança das suas finanças.

Como manter sua conta segura

- **Prefira um celular exclusivo para transações bancárias:** Manter um celular separado apenas para manter suas principais contas bancárias pode ser uma medida eficaz para reduzir riscos de invasão e golpes. Esse celular deve preferencialmente ficar em casa, além de evitar a utilização dele com outros aplicativos ou sites que possam comprometer a segurança.

- **Reduzir limites de transações:** Ajuste o limite do PIX e de outras transações para um valor mais baixo. Assim, é possível mitigar o impacto de possíveis fraudes ou crimes. Em caso de acesso indevido, os danos serão limitados ao valor estipulado.

- **Utilize contas secundária para pequenas transações:** Para transações pequenas e cotidianas, como compras em lojas menores e pagamentos de pequenas contas, considere utilizar uma conta secundária. Essa conta pode ter saldo limitado, minimizando os riscos caso ela seja comprometida.

- **Habilite proteções adicionais na conta:** A maioria dos bancos oferecem diversas camadas de segurança que podem ser ativadas para proteger sua conta. Essas proteções incluem autenticação em dois fatores, notificações no celular, reconhecimento facial e bloqueio temporário de cartões. Certifique-se de habilitá-las para aumentar sua segurança.

Conclusões

Em um mundo cada vez mais digital, tornou-se uma prioridade essencial a segurança online. Desde identificar ofertas imperdíveis que são, na verdade, armadilhas, até reconhecer ligações fraudulentas e proteger cartões, é crucial adotar práticas para minimizar os riscos de fraude. Manter o BP em segurança, utilizar dispositivos e conexões seguras para transações bancárias e estar atento a golpes em redes sociais são passos fundamentais para preservar a segurança financeira.

Essa campanha tem como objetivo educar e conscientizar sobre as diversas ameaças que enfrentamos diariamente. Ao seguir as práticas recomendadas, como reduzir o limite do PIX, utilizar um celular exclusivo para transações bancárias e habilitar proteções adicionais nas suas contas, você fortalece suas defesas contra os perigos cibernéticos. A prevenção é a melhor forma de evitar prejuízos e garantir que você possa se manter conectado com maior confiança e segurança.

Então, que tal aplicar essas dicas e garantir uma maior segurança na sua rotina, evitando golpes e fraudes?

Onde Obter Orientação?

A Marinha possui um compêndio normativo completo sobre segurança, o que inclui orientações sobre boas práticas de Segurança da Informação. As responsabilidades e orientações aos usuários da RECIM podem ser encontradas na DGMM-0540 – Normas de Tecnologia da Informação da Marinha. Além disso, a DCTIMARINST Nº 31-06 – Plano de Gestão de Incidentes Cibernéticos apresenta orientações sobre responsabilidades e como reportar incidentes que estejam correlacionados à MB.