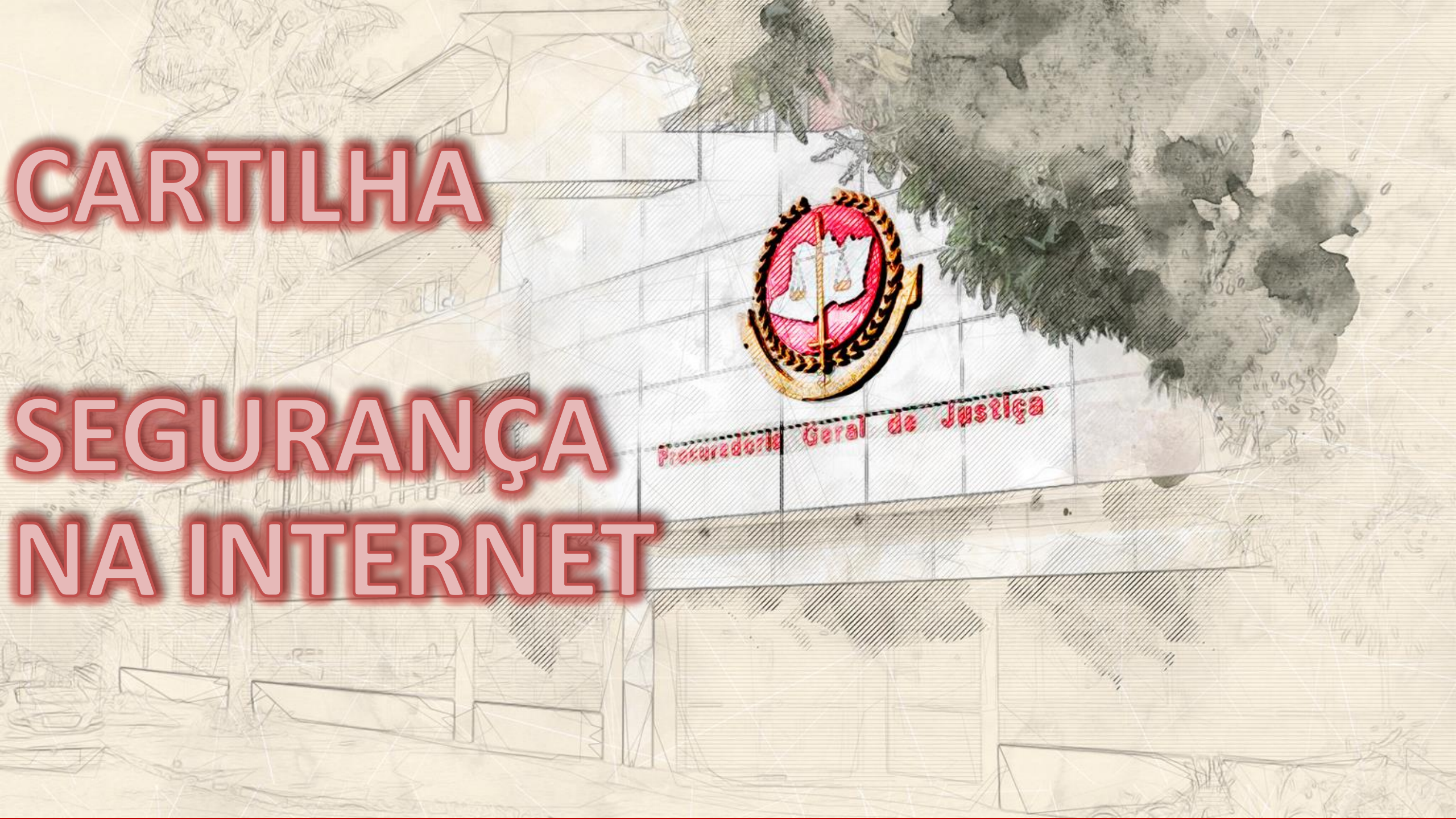
CARTILHA

SEGURANÇA NA INTERNET



Procurador-Geral de Justiça do Amazonas

Dr. Alberto Rodrigues do Nascimento Júnior

Subprocurador-Geral de Justiça para Assuntos Jurídicos e Institucionais

Dr. Nicolau Libório dos Santos Filho

Subprocurador-Geral de Justiça para Assuntos Administrativos

Dr. Géber Mafra Rocha

Corregedora-Geral

Dra. Sílvia Abdala Tuma

Ouvidora-Geral

Dra. Jussara Maria Pordeus e Silva

Secretária-Geral do Ministério Público do Estado do Amazonas

Dra. Lílian Maria Pires Stone

COMITÊ GESTOR DE POLÍTICAS DE SEGURANÇA INSTITUCIONAL

Presidente do CGPSI

Dr. Nicolau Libório dos Santos Filho

Membros:

Procurador de Justiça

Dr. Públio Caio Bessa Cyrino

Procuradora de Justiça

Dra. Karla Fregapani Leite

Promotor de Justiça

Dr. André Lavareda Fonseca

Promotor de Justiça

Dr. George Pestana Vieira

Assessor de Segurança Institucional

Paulo Emilio Vieira de Melo – TC PM

EQUIPE DE ELABORAÇÃO E REVISÃO

Assessor de Segurança Institucional

Paulo Emilio Vieira de Melo – TC PM

Assessor Adjunto de Segurança Institucional

Dã Cesar Tavares de Azevedo – Maj PM

COLABORAÇÃO

Chefe do Centro de Estudos e Aperfeiçoamento Funcional

Dr. Darlan Benevides de Queiroz

Assessora de Comunicação

Daniela Bragança Macedo

Chefe do Núcleo de Segurança do TRT 11

Ailton Luiz dos Santos – Maj PM

Chefe da Seção de Gestão Risco de Segurança do TRT 11

Gutemberg Watson Gomes – Sgt PM

APRESENTAÇÃO

Cada vez mais as pessoas têm utilizado o meio virtual para se comunicar, realizar compras, enviar e receber dados e até mesmo para se relacionarem. Essa maior exploração das ferramentas tecnológicas também atrai a atenção de criminosos, que visam justamente atuar nas oportunidades e vulnerabilidades criadas por esses usuários. Dessa forma, é fundamental que Membros e Servidores do MPAM, bem como a população em geral, tenham conhecimentos básicos nessa temática e possam adotar comportamentos de proteção contra os principais golpes aplicados no cotidiano.

SUMÁRIO

Engenharia Social

Engenharia Social é a habilidade de conseguir acesso à informações confidenciais sobre nome, senhas, detalhes do cartão de crédito, clonagens ou a áreas importantes de uma pessoa ou instituição através de habilidades de persuasão.

Fonte: Adobe Stock

Dicas de segurança

- Orientes pessoas próximas e familiares sobre o perigo de fornecer informações sensíveis, como dados pessoais, que são solicitadas na rua, por telefone ou pela internet;
- Desconfie de mensagens que pedem confirmação de dados pessoais ou informações sensíveis sem que você tenha solicitado;
- Não clique em links desconhecidos em SMS, e-mails ou publicações em redes sociais.
- Não clique em banners de propagandas não confiáveis.
- Se seu celular foi extraviado, solicite o imediato bloqueio de seu número junto à operadora e realize o procedimento para “apagar” o dispositivo;
- Elabore sempre senhas “fortes” para proteger suas contas e seus dispositivos, sejam pessoais ou institucionais, buscando ativar a verificação em duas etapas.

Phishing (Pescaria)

Phishing consiste em ludibriar as pessoas levando-as a compartilhar informações confidenciais como senhas e número de cartões de crédito. Normalmente os golpistas lançam uma isca, em regra algo atrativo e vantajoso, para que assim possam “pescar” os dados sensíveis das vítimas.

Fonte: Adobe Stock

Dicas de segurança

- Lembre-se de que phishing é um ataque oportunista. Não clique em links desconhecidos em mensagens de SMS, e-mails, WhatsApp ou publicações em redes sociais.
- Desconfie de propostas vantajosas demais, principalmente quanto à possibilidade de e-mails falsos enviados às suas caixas de entrada. Não abra mensagens de remetentes desconhecidos.
- Em ligações oriundas de telemarketing, não forneça nem “confirme” seus dados pessoais, principalmente informações de login e senha.
- Uma defesa das mais eficazes contra as iscas está em sua educação. Cada um de nós deve se esforçar para ter uma forte cultura de segurança em nossos ambientes de trabalho e em casa.
- Não baixe arquivos automaticamente, nem faça downloads de arquivos desnecessários, assim como deve-se evitar a execução de arquivos não solicitados.

Clonagem do Whatsapp

Neste tipo de ação os golpistas cadastram o número da vítima em um outro aparelho e, para concluir a operação, constroem uma situação hipotética para conseguirem o código de segurança que é enviado para a vítima via SMS. Normalmente simulam um atendimento ao cliente, informando uma necessidade de atualização ou confirmação de dados. Uma vez concretizada a ação e de posse das conversas e contatos da vítima, os criminosos passam a pedir dinheiro se passando pela pessoa atacada.

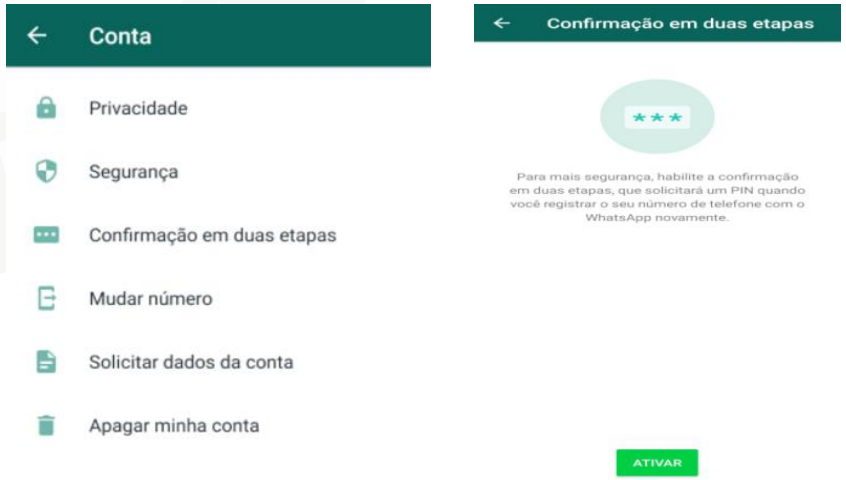
Fonte: Adobe Stock

Dicas de segurança

Uma das formas de diminuir as chances de golpes via WhatsApp, como clonagem e falso perfil, é utilizando a ferramenta de confirmação em duas etapas. Como, então, proceder?

No menu de configurações, acesse Conta e, em seguida, Confirmação em Duas Etapas. Ao clicar em Ativar, insira o PIN de seis dígitos e um e-mail para recuperação de senha.

Pronto! É importante não fornecer, sob nenhum pretexto, seu PIN ou código SMS a ninguém. Assim, seus dados estarão mais seguros.



Falso Boleto

Consiste no direcionamento da vítima para falsas páginas da web, nas quais é induzida a realizar downloads de boletos forjados e quase idênticos aos originais. Ao realizar o pagamento, a vítima direciona seus recursos à conta de fraudadores e continua com a dívida junto ao credor original.

Fonte: Adobe Stock

Dicas de segurança

- Não realize pagamentos de boletos que não foram solicitados por você. Consulte seu gerente do banco sempre que o estado de dúvida persistir.
- Antes de finalizar o pagamento de um boleto, confira se o beneficiário é o mesmo que consta no documento.
- Não deixe de conferir os demais dados do boleto, como valor, data de vencimento, emissor, visando ter certeza de que está pagando corretamente.
- Confira o código do banco constante no boleto (três primeiros dígitos do código de barras).
- Sempre que precisar de outra via para pagamento, faça a solicitação no canal oficial da empresa credora.

Intermediador de Vendas

Nesse tipo de ação criminosa, muito comum em portais de negociação de automóveis como OLX, Webmotors e Icarros, os golpistas constroem um enredo envolvente, de modo que as vítimas, uma interessada em vender o bem, e outra interessada em comprar, sempre imaginam que estão tratando com um intermediador. Este intermediador, na verdade o criminoso, prometendo vantagens financeiras para ambas as partes, e utilizando de argumentos convincentes, faz com que as vítimas não conversem entre si, evitando, dessa maneira, que o golpe seja descoberto. Dessa forma, o intermediário consegue receber o valor do bem como se fosse o proprietário ou estivesse agindo em nome dele.

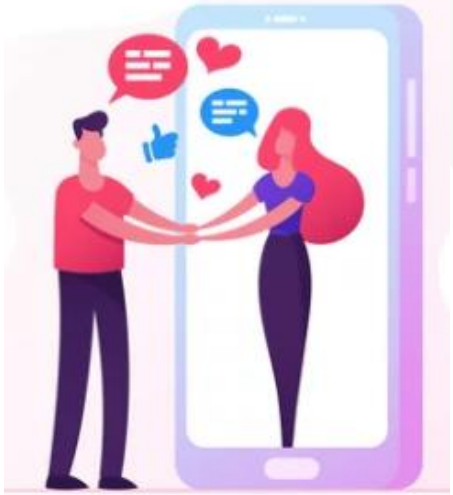
Fonte: Adobe Stock

Dicas de segurança

- Durante uma negociação retire o máximo de dúvidas possíveis sobre a propriedade e procedência de um bem.
- Sempre desconfie quando alguém pede sigilo em uma negociação, em troca de desconto.
- Jamais conclua um pagamento com a promessa de garantir a compra do bem.
- Somente entregue o bem após confirmar que o devido pagamento foi creditado em sua conta bancária
- Desconfie de produtos ou bens que estejam sendo oferecidos por valores muito abaixo dos normalmente praticados no mercado.

Extorsão Amorosa

A partir de ações em sites ou aplicativos de encontros e namoro, os golpistas buscam iniciar um relacionamento virtual com a vítima. À medida em que a relação amorosa evolui e se consolida, o criminoso executa comportamentos para deixar a vítima cada vez mais envolvida emocionalmente. Atingindo um patamar desejado, começa a criar situações que viabilizam pedidos de dinheiro, como simulação de doenças, pagamentos de dívidas, compras de remédios. Há casos, ainda, em que os bandidos utilizando fotos íntimas da pessoa, passa a exigir somas em dinheiro para não fazer a divulgação.



Fonte: Adobe Stock

Dicas de segurança

- Ao conhecer uma pessoa virtualmente, é importante, com segurança, tentar saber se realmente existe ou se não passa de um perfil fake.
- Não é prudente enviar fotos ou vídeos íntimos a ninguém, quanto mais à pessoas conhecidas em ambiente virtual.
- Jamais transfira dinheiro para um suposto namorado virtual, por mais triste que seja o caso relatado.
- Não compartilhe seus dados pessoais ou de cartão de crédito com seu relacionamento virtual, mesmo com a promessa de devolução do valor.
- Ao ser vítima desse tipo de prática, mantenha as conversas salvas, para servirem de prova, e procure de imediato a Delegacia de Polícia.

Máquina de pagamento quebrada

Ação delituosa se inicia no momento da entrega do pedido, após o cliente ter solicitado um produto ou serviço via aplicativo, em regra. Nesse caso, o golpista apresenta à vítima uma máquina para pagamento com o visor quebrado, sem que seja possível identificar o valor que está sendo inserido. Pode também ocorrer quando a compra já foi paga no aplicativo e, para isso, o entregador simula um problema com o pagamento e induz a vítima a passar o cartão novamente.

Fonte: Adobe Stock

Dicas de segurança

- É importante sempre conferir o valor da compra antes de finalizar o pagamento.
- Caso a máquina esteja danificada, não aceite o equipamento para fechar a compra.
- É aconselhável, nas compras virtuais, realizar o pagamento pelo próprio aplicativo, evitando, desse modo, tais golpes.
- Caso tenha pago o valor por aplicativo, não aceite novas cobranças feitas na hora da entrega.

Orientações Gerais

Por mais diversos que sejam, os inúmeros golpes existentes em ambientes virtuais guardam alguns pontos em comum. Os golpistas que atuam nesse campo aproveitam simples distrações e comportamentos ingênuos das vítimas. A adoção de algumas medidas básicas, porém eficazes, pode dificultar a ação dos criminosos e proteger melhor o seu patrimônio.

Fonte: Adobe Stock

Dicas de segurança

- Não acredite em propostas vantajosas demais. Desconfie de produtos oferecidos por valores abaixo dos usuais.
- Não clique em links suspeitos nos e-mails, WhatsApp ou redes sociais, pois podem ser a porta de entrada para seus dados.
- Não aceite fornecer seus dados pessoais ou de cartão de crédito em supostas confirmações e atualizações, seja por telefone ou formulários virtuais.
- Cubra o código de segurança dos seus cartões (3 dígitos no verso) com um adesivo.
- Não transfira valores para pessoas que você conhece apenas no mundo virtual.
- Retenha suas senhas com o máximo cuidado. Não as deixe em blocos de nota no celular ou computador. Prefira utilizar senhas fortes e autenticação em duas etapas.


Procuradoria Geral de Justiça