Série GOLPES DIGITAIS

Veja todos os itens/elementos da série em:

http://www.aldemario.adv.br

GOLPES DIGITAIS 1

Pelo menos 71% dos brasileiros já sofreram alguma tentativa de fraude eletrônica, mostra pesquisa publicada em junho de 2023 pela Nord Security, empresa de segurança digital.

Sinais de alerta para desconfiar de um golpe:

PEDIDOS DE SENHAS (em ligações telefônicas e mensagens recebidas)

URGÊNCIA EM PEDIDOS

PREÇO BAIXO (considerando a média do mercado)

ERROS DE PORTUGUÊS

PAGAMENTOS ANTECIPADOS (para liberação de produtos e serviços)

PAGAMENTOS A TERCEIROS (pessoas estranhas ao negócio realizado)

Fonte: Tilt UOL

NÃO ATENDER CHAMADAS DE NÚMEROS DESCONHECIDOS (NÃO INTEGRANTES DA AGENDA DE CONTATOS)

Não atender chamadas telefônicas de números desconhecidos é uma prática cada vez mais comum para evitar spam, telemarketing e possíveis golpes.

Em regra, as tentativas legítimas de contato serão realizadas por intermédio de aplicativos de mensagens instantâneas, como o WhatsApp.

GOLPES DIGITAIS 3

SENHAS FORTES E ÚNICAS

I. Utilize senhas complexas, com letras maiúsculas e minúsculas, números e símbolos.

II. Crie senhas usando uma frase.
Exemplo: “A vida é uma aventura” > Av1d@E1Av3ntUr@

III. Evite datas de nascimento, nomes próprios, nomes de empresas, sequências fáceis de adivinhar e palavras encontradas em dicionários.

IV. Evite usar a mesma senha em diferentes contas.

V. Troque as senhas regularmente.

DADOS PESSOAIS, QRcodes E CÓDIGOS DE BARRA

Inutilizar nomes, telefones, endereços, QR codes e códigos de barras em encomendas recebidas é uma prática recomendada por motivos de segurança e privacidade.

Esses dados podem ser usados para “roubo” de identidade, golpes e ações de engenharia social.

Esses elementos devem ser riscados ou rasgados.

CONSULTAS PERIÓDICAS AO SERASA

Seus dados pessoais podem ser utilizados para gerar operações ilegítimas em seu nome (como empréstimos bancários).

Consulte periodicamente seu CPF no site da SERASA (serasa.com.br) e descubra se existem restrições no seu nome, protestos em cartórios e outras informações.

GOLPES DIGITAIS 6

BOLETOS BANCÁRIOS

I. Verifique o nome do favorecido/beneficiário.

II. Certifique-se de que o valor do boleto no corpo do documento corresponde ao valor que aparece ao digitar o código de barras.

III. Verifique, com cuidado redobrado, a origem dos boletos recebidos por e-mail.

IV. Cadastre-se no DDA (Débito Direto Autorizado) do seu banco. O DDA mostra boletos emitidos em seu CPF/CNPJ, o que ajuda a evitar fraudes com documentos não registrados (desde 2018, os boletos devem ser registrados pelos bancos).

GOLPES DIGITAIS 7

A LIGAÇÃO TELEFÔNICA DE SEU BANCO PODE NÃO SER DO SEU BANCO

I. O golpe que se passa por ligação do seu banco é uma fraude muito comum. Golpistas se fingem de funcionários do banco para obter informações pessoais, como senhas e dados bancários, solicitar transferências e pagamentos ou indicar supostos procedimentos de segurança.

II. Os golpistas ligam para a vítima usando um número que simula o do banco. Eles podem usar táticas de urgência ou criar uma sensação de emergência para manipular as vítimas.

III. Não forneça dados. Não faça transferências. Não siga instruções de acesso a links ou aplicativos.

IV. Entre em contato com seu banco diretamente para verificar se existe alguma pendência a ser equacionada.

GOLPES DIGITAIS 8

CELULAR PERDIDO, FURTADO OU ROUBADO

I. Providencie o bloqueio e rastreamento do aparelho por intermédio dos sites dos fabricantes.

II. Faça o bloqueio do IMEI (código numérico único de cada celular) e da linha telefônica. Entre em contato com sua operadora. Você pode utilizar o aplicativo "Celular Seguro" do Ministério da Justiça e Segurança Pública.

III. Altere todas as senhas dos serviços instalados no celular.

IV. Notifique seu(s) banco(s).

V. Registre um Boletim de Ocorrência na Polícia Civil.

VI. Informe familiares e amigos.

GOLPES DIGITAIS 9

VÍDEOS E ÁUDIOS FALSOS DE PERSONALIDADES, JORNALISTAS DE TV E POLÍTICOS (COM USO DE INTELIGÊNCIA ARTIFICIAL)

I. Não acesse sites ou aplicativos indicados nesses vídeos e áudios

II. Não preencha formulários e não forneça dados pessoais solicitados a partir desses vídeos e áudios

III. Desconfie de promoções, brindes, descontos e qualquer vantagem (em dinheiro ou não) indicados nesses vídeos e áudios

GOLPES DIGITAIS 10

PERFIS HIPER-REALISTAS DE MULHERES CRIADOS POR INTELIGÊNCIA ARTIFICIAL

I. Vídeos dirigidos a homens, em regra,
com mais 50 anos e emocionalmente carentes

II. Simulam mulheres bonitas e atraentes bem-sucedidas ou extremamente vulneráveis

III. Invariavelmente, são solicitadas transferências financeiras em troca do envio de fotos ou vídeos, para pagamento de contas/despesas atrasadas ou para auxílio em situações de doenças na família

GOLPES DIGITAIS 11

DESCONFIE DE LINKS RECEBIDOS

I. Links maliciosos são uma das ferramentas mais comuns e eficazes utilizadas por golpistas.

II. A desconfiança em relação a qualquer link que você receba, seja por e-mail, mensagem de texto, redes sociais ou até mesmo em sites aparentemente legítimos, é uma das principais defesas contra fraudes e roubos de dados.

III. Atenção para: a) remetente desconhecido ou suspeito; b) erros de ortografia e gramática; c) tom de urgência ou “ameaça”; d) solicitação de informações pessoais; e) link que não corresponde ao texto e f) domínio incomum do site indicado no link (ex.: brasilbanco.com)

IV. Adote este cuidado básico: antes de clicar, passe o mouse sobre o link para ver o destino real. Se estiver em um dispositivo móvel, mantenha o dedo pressionado sobre o link por alguns segundos (sem soltar rapidamente para não clicar) para que o endereço de destino apareça.

AUTENTICAÇÃO DE DOIS FATORES

I. A autenticação de dois fatores (2FA), também conhecida como verificação em duas etapas, é um relevante recurso de segurança que acrescenta uma camada extra de proteção ao acesso a contas e sistemas online. Além da senha tradicional, a 2FA exige um segundo elemento de identificação, como um código gerado por um aplicativo ou dispositivo, ou dados biométricos.

II. É importante ativar a autenticação de dois fatores sempre que disponível. Ela aumenta significativamente a segurança das contas e dados pessoais.

GOLPES DIGITAIS 13

GOLPE DO CARTÃO POR APROXIMAÇÃO

I. O pagamento por aproximação ocorre quando um cartão com a tecnologia NFC (Near Field Communication ou comunicação por aproximação) chega bem próximo de uma maquininha de pagamento.

II. O golpe consiste em colocar um valor na máquina e tentar encostar nos cartões das vítimas (guardados em bolsos ou bolsas) sem que elas percebam. Inúmeras ocorrências envolvem o uso de alguém para distrair a atenção da vítima.

III. A tecnologia NFC não requer o uso de senha. Assim, o valor pode ser processado sem a vítima identificar imediatamente a operação.

IV. Os cuidados recomendados são: a) desativar o pagamento por aproximação; b) limitar o valor de operações sem senha; c) usar carteira digital no celular; d) ativar as notificações de transações financeiras e e) utilizar protetor de cartão que bloqueia a transmissão de dados.

GOLPES DIGITAIS 14

DESCONFIE DE TODO VÍDEO QUE BUSCA CONVENCER DE ALGO

“Em vídeos com estética de documentário, cortes suaves, drones imaginários e trilha sonora épica, surgem cenas que antes habitavam fóruns conspiracionistas e comentários de rodapé: uma muralha de gelo na Antártida, reptilianos escapando do subsolo, naves pairando sobre cidades, pirâmides escondidas na Amazônia, a Arca de Noé intacta, gigantes construindo civilizações. Tudo com aparência de realidade. Tudo com tecnologia de ponta.

Durante anos, o que impedia essas histórias de ganharem força era a estética. Os próprios conspiracionistas reclamavam que seus vídeos eram sempre em baixa resolução. A piada era automática: “com tanta tecnologia no mundo, ninguém filma um disco voador em HD?”. Isso mudou. Com ferramentas como o Veo 3, a nova IA de vídeos do Google, qualquer pessoa pode transformar delírios em vídeo com qualidade cinematográfica. Basta digitar: ‘crie um vídeo realista de um avião da NASA sobrevoando estátuas alienígenas em Ratanabá’, e o vídeo aparece. Em segundos. Com luz, sombra, narração pausada e tudo que um conteúdo viral precisa. A IA não cria provas. Ela cria provas necessárias para convicções existentes” (Estadão, 30/07/2025).

GOLPES DIGITAIS 15

GOLPE DO FALSO ADVOGADO

"o golpe do falso advogado ocorre especialmente em virtude de demandas judiciais, pois os golpistas têm acesso aos dados insertos nos processos judiciais, que são públicos./O golpista entra em contato com os clientes ou partes, se passando pelo advogado contratado ou pelo respectivo escritório, e solicita transferências via PIX, alegando que o pagamento prévio de um valor é necessário para liberar um suposto crédito existente no processo" (Cartilha da OAB/SP).

Cuidados:

I - Desconfie de ligações telefônicas ou mensagens de pessoas se passando por advogados ou representantes de escritórios, especialmente se solicitarem pagamentos adiantados (PIX ou transferência bancária).

II - Entre em contato diretamente com o advogado ou escritório de advocacia apontado na comunicação recebida. Utilize os dados de contato oficiais (no site, no contrato de honorários, no cartão de visita, etc).

III - A Ordem dos Advogados do Brasil (OAB) possui a plataforma ConfirmaADV (confirmadv.oab.org.br) e o acesso ao Cadastro Nacional de Advogados (cna.oab.org.br) que permitem confirmar a identidade de um advogado.

GOLPES DIGITAIS 16

GOLPE DA INDENIZAÇÃO PAGA PELO GOVERNO FEDERAL

I. “É falso que brasileiros serão indenizados em até R$ 20 mil pelo governo federal por conta de um suposto vazamento de dados. As peças de desinformação que fazem essa alegação direcionam usuários a sites que falsificam a identidade visual do portal gov.br para aplicar um golpe” (aosfatos.org).

II. São falsos: a) o programa “Indeniza Brasil”; b) o “Processo Indenizatório do Governo” e c) variações dessas últimas denominações.

III. Não forneça dados. Não faça transferências (não existe a “taxa transacional”). Não siga instruções de acesso a links ou aplicativos.

IV. “Como o pagamento é feito por Pix, eventuais vítimas da fraude podem recorrer ao MED (Mecanismo Especial de Devolução), sistema criado pelo Banco Central para reparar danos gerados por fraude com o uso da tecnologia” (aosfatos.org).

V. “Não acredite em promessas em que há necessidade de pagar taxas para efetuar saques e sempre consulte a procedência dos programas no site oficial do governo federal” (aosfatos.org).

GOLPES DIGITAIS 17

RECEBEU LIGAÇÃO TELEFÔNICA DE UM NÚMERO IGUAL OU COM OS PRIMEIROS DÍGITOS PARECIDOS COM O SEU?

I. “O número que efetua a ligação é outro. Ele é inserido em serviços de chamadas pela internet (VoIP), que permitem escolher o número que será mostrado no destino. Como os golpistas usam o telefone da vítima como ‘disfarce’, é ele quem aparece no visor”.

II. “Essa tentativa de golpe, que tem sido cada vez mais utilizada, é conhecida como ‘spoofing’ (...) Ela é apenas um artifício de engenharia social que golpistas usam para ludibriar vítimas, atiçando-as pela curiosidade".

III. “Nunca forneça nome de usuário ou senhas por telefone e só faça ligações para números oficiais. Caso você precise entrar em contato com alguma empresa, use o número de telefone oficial da companhia. Não ligue para números fornecidos durante ligações suspeitas”.

Fonte: TiltUOL (uol.com.br)

GOLPES DIGITAIS 18

NÃO ALIMENTE MODELOS DE INTELIGÊNCIA ARTIFICIAL COM INFORMAÇÕES SENSÍVEIS

I. Jamais alimente um modelo de Inteligência Artificial - IA (ChatGPT, Gemini, etc) com dados e informações sensíveis. Esse cuidado abrange: senhas, dados bancários, números de documentos (CPF, RG e outros) e qualquer informação pessoal que possa ser usada como fator de identificação.

II. A maioria dos modelos de IA adotam medidas de segurança e políticas de privacidade, mas não há garantia de que esses dados estarão totalmente protegidos.

III. Dados e informações sensíveis podem ser expostos acidentalmente, acessados por terceiros mal-intencionados ou, em certos casos, armazenados nos servidores para desenvolver/treinar o modelo de IA.

GOLPES DIGITAIS 19

GOLPE DO PAGAMENTO ENVOLVENDO TRANSPORTADORAS DE ITENS COMPRADOS VIA INTERNET

I. Os golpistas têm usado o nome de transportadoras para enganar consumidores com mensagens falsas no WhatsApp e SMS.

II. São pedidas atualizações de endereços ou pagamentos de taxas, sob pena de perda dos bens adquiridos.

III. Para se proteger, não clique em links ou botões, nem abra anexos de e-mails de origem desconhecida. Não forneça dados pessoais.

IV. Entre em contato diretamente com o vendedor do produto.

V. Ao colocar o cursor em cima de links e botões (sem clicar) é possível identificar o endereço para onde aponta o elemento em questão. Em regra, aparecem domínios completamente diferentes daqueles que são indicados expressamente na mensagem.

BOMBARDEIO DE AMOR (LOVE BOMBING)

I. Utiliza aplicativos de relacionamento ou perfis falsos em redes sociais (simulando até mesmo pessoas famosas).

II. O golpista se mostra totalmente disponível emocionalmente para se envolver, sem medo de compromisso.

III. O golpista demonstra um interesse intenso e acelera a relação, declarando “amor” rapidamente e criando uma sensação de “alma gêmea”.

IV. Depois do momento de completo envolvimento emocional é quando os pedidos de dinheiro começam, normalmente como ajudas (para fechar negócios ou tratar doenças), investimentos imperdíveis e taxas para desbloquear o envio de presentes.

GOLPES DIGITAIS 21

FUNÇÃO “NÃO PERTURBAR” EM CELULARES

I. A função "não perturbar" é uma configuração de celulares que silencia notificações, chamadas telefônicas e outros alertas para evitar interrupções. Foi concebida para uso em momentos que exigem maior concentração (reuniões, aulas, eventos, etc).

II. A função “não perturbar” permite personalizar quais tipos de interrupções podem passar, como chamadas telefônicas de contatos já registrados no aparelho.

III. Trata-se de uma opção mais “radical” para não receber ligações telefônicas de golpistas e vendedores.

IV. Para ativar a função “não pertubar” em iPhones:
Ajustes > Foco > Não perturbe.

V. Para ativar a função “não perturbar” em androids (Samsung, Motorola, Xiaomi, etc):
Configurações > Notificações > Não perturbar.

GOLPES DIGITAIS 22

AINDA SOBRE SENHAS

“A cibersegurança se tornou um dos temas mais discutidos no mundo digital, especialmente porque as senhas são a primeira defesa contra hackers. Elas protegem seus dados e só permitem acesso com as credenciais corretas. Mas muita gente ainda cria senhas fracas e fáceis de descobrir.

Como resultado do mau uso das senhas, os usuários podem ser vítimas de roubos ou fraudes digitais, evidenciando que a maioria ainda usa combinações simples — e, muitas vezes, a mesma senha para vários acessos.

Uma pesquisa de Troy Hunt sobre cibersegurança analisou mais de 100 milhões de senhas vazadas e descobriu que as pessoas utilizam cinco senhas muito simples e óbvias.

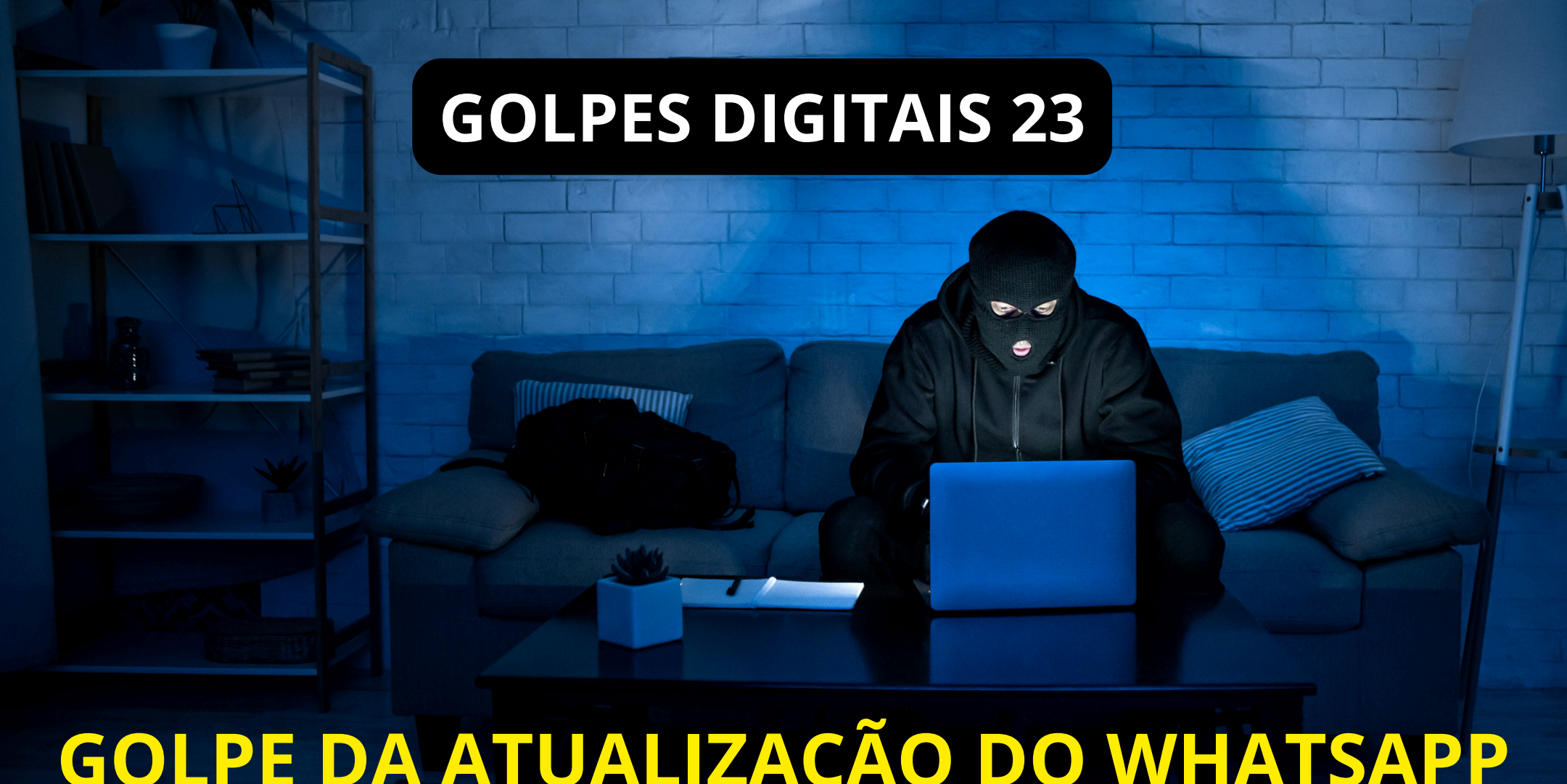
Segundo o estudo, **a combinação “123456” é usada por mais de seis milhões de usuários no mundo**, enquanto **“123456789” é a alternativa mais comum para dois milhões de internautas**.

O que mais chamou atenção do autor é que **algumas pessoas ainda usam “111111”** ou **palavras como “password” e “qwerty”** - seis primeiras letras da linha superior do teclado, fácil de digitar - para proteger contas virtuais ou celulares, facilitando o trabalho de cibercriminosos.

Para reduzir o risco de violação de segurança e evitar ataques de terceiros, é importante criar senhas com 12 caracteres ou mais, **combinando letras maiúsculas, minúsculas, números e símbolos.**

Outra recomendação é **usar senhas diferentes para cada conta** e incluir palavras incomuns, já que criminosos tentam adivinhar combinações usando expressões de dicionário.

Uma das opções mais eficazes é recorrer a letras de músicas, citações ou frases populares, adicionando caracteres especiais para tornar a senha mais segura e fácil de lembrar” (fonte: oglobo.globo.com).



GOLPE DA ATUALIZAÇÃO DO WHATSAPP

I. O usuário recebe uma mensagem falsa contendo um link com a expressão “Atualizar o WhatsApp”.

II. Ao clicar no link, o celular pode ser clonado e viabilizado o acesso a dados pessoais e informações bancárias.

III. Não clique em links recebidos pelo WhatsApp, especialmente de números desconhecidos.

IV. Atualize os Apps (aplicativos) apenas pelas lojas oficiais (Google Play e App Store).

GOLPES DIGITAIS 24

DESCONFIAR E PERGUNTAR

I. “Os golpistas estão mais espertos do que muito e-commerce. São os únicos que nunca ficam sem estoque: sempre têm um golpe novo para oferecer. Não atrasam entrega, não cancelam pedido, não avisam que “o produto está em falta no fornecedor”. Criam site bonito, mandam mensagem simpática, inventam urgência e servem a fraude como se fosse promoção relâmpago” (Cora Rónai).

II. “No fundo, só tem um truque que funciona contra isso: **desconfiar sempre**. É cansativo, eu sei — ninguém aguenta viver em estado de alerta permanente. Mas, na vida digital, a desconfiança é o antivírus que nunca falha” (Cora Rónai).

III. A escritora Cora Rónai destacou a primeira das duas atitudes necessárias para lidar com o frenético, útil e perigoso mundo digital. É preciso desconfiar (acordado e dormindo, até porque os celulares ficam ligados).

IV. A segunda conduta fundamental é **perguntar** para alguém “mais bem informado” acerca de toda situação nova (diferente daquelas que você já está acostumado a lidar e se repetem periodicamente).

GOLPES DIGITAIS 25

CRIMES DIGITAIS SUPERAM CRIMES FÍSICOS

I. “Os criminosos modernos, imersos no mundo da tecnologia, já não precisam mais de máscaras ou armas para agir. Cada vez mais, os golpes estão acontecendo atrás de telas, no ambiente virtual. Pelo menos é isso o que afirma o Anuário Brasileiro de Segurança Pública de 2025, divulgado pelo Fórum Brasileiro de Segurança Pública. Para se ter uma ideia da gravidade do problema, em 2024, o Brasil registrou quatro estelionatos virtuais por minuto. Isso revela uma mudança radical nos perfis tradicionais de crime: **enquanto roubos e homicídios caem, os golpes e fraudes digitais aumentam**, o que expõem a fragilidade da população diante desse novo tipo de violência”.

II. “Nos últimos anos, os crimes digitais deixaram de ser exceção para se tornar rotina na sociedade. As estatísticas do Anuário Brasileiro de Segurança Pública mostram que **as fraudes praticadas em ambientes virtuais já ultrapassam modalidades tradicionais de crime, como roubos e furtos**. Em 2024, foram mais de 2,2 milhões de registros de estelionato digital, um número 50 vezes maior que o total de homicídios no mesmo período. A queda nos crimes "clássicos", como roubos de celulares e assaltos em geral, reforça a ideia de que a criminalidade está migrando para o mundo virtual, onde as chances de punição são menores e as oportunidades de enganar vítimas são muito maiores”.

Fonte: terra.com.br

GOLPES DIGITAIS 26

DESCONFIAR E PERGUNTAR II

"Fernanda Paes Leme, 42, relatou hoje (23) nas redes sociais uma tentativa de **golpe envolvendo a ativação do seu WhatsApp em outro aparelho**.

Nos stories, a atriz contou que **recebeu uma mensagem solicitando a inserção de um código de verificação para um 'novo dispositivo**'. Paes Leme disse que não havia solicitado, alegando que não havia trocado de celular e nem estava com seu computador.

'Cara, eu tô recebendo uma mensagem pedindo pra eu inserir o código pro WhatsApp num dispositivo novo. Só que eu não tenho nenhum dispositivo novo. Tão querendo clonar alguma coisa minha, é isso? É número clonando um número? **Alguém me explica? Alguém que sabe aí, me explica?' Questionou Fernanda aos seguidores**.

Pouco depois, a apresentadora retornou às suas publicações para avisar que já havia recebido orientações dos seguidores e confirmar que se tratava de um golpe. **'Todo mundo me respondeu aqui. É golpe, é golpe, é golpe. Não passa nada, não muda nada, não escreve nada, não digita nada, é golpe. Não vou cair**'". Fonte: uol.com.br