“Não Clique”: Cultura de Segurança para Funcionários e Terceiros

Estratégias de Prevenção a Incidentes de Segurança Cibernética

Sumário

Módulo 1. Introdução

Sabemos que muitos incidentes de segurança não ocorrem por falhas técnicas, mas sim por descuidos ou desconhecimento dos usuários no dia a dia. Em um cenário em que golpes exploram pressa, curiosidade e boa-fé, o comportamento certo, no momento certo, evita prejuízos financeiros, paralisação de operações e danos à reputação.

Este trabalho foi especialmente criado para desenvolver, em todos os colaboradores, uma cultura de segurança baseada em desconfiança saudável, confirmação por canais oficiais e cumprimento de protocolos. É importante promover uma cultura de segurança da informação dentro da instituição, como responsabilidade de todos. Afinal, a tecnologia, por mais avançada que seja, não substitui a atenção e o bom senso humano.

Em um cenário cada vez mais digital e interconectado, as instituições enfrentam desafios crescentes para proteger seus ativos, informações e reputação.

As ameaças virtuais não se limitam mais a ataques sofisticados contra grandes corporações: hoje, qualquer organização pode se tornar alvo de tentativas de fraude, roubo ou sequestro de dados, pagamentos redirecionados ou sabotagem. Nesse contexto, a conscientização e a capacitação dos colaboradores deixam de ser opcionais para se tornarem elementos estratégicos de defesa.

Ao investir na formação de seus colaboradores, a instituição reduz significativamente as chances de sofrer ataques bem-sucedidos dos fraudadores, como phishing, engenharia social ou instalação de softwares maliciosos. Cada funcionário treinado se torna um elo mais forte na corrente de proteção, capaz de identificar sinais de perigo e agir preventivamente. Esse fortalecimento coletivo não apenas preserva dados e sistemas, mas também protege a imagem e a credibilidade da organização perante clientes, parceiros e o mercado.

Além da mitigação de riscos imediatos, o curso contribui para criar uma cultura corporativa mais responsável e alinhada às boas práticas de segurança da informação. Isso favorece a conformidade com leis e regulamentos, como a Lei Geral de Proteção de Dados (LGPD), e demonstra comprometimento com padrões éticos e de governança. Em um ambiente de negócios onde a confiança é um ativo valioso, essa postura representa um diferencial competitivo importante.

Portanto, este curso não é apenas um treinamento técnico, mas um **investimento estratégico** em pessoas, processos e na própria sustentabilidade da instituição. Ao unir conhecimento, atenção e responsabilidade, é possível transformar cada colaborador em um agente ativo de proteção, criando barreiras mais sólidas contra as ameaças e garantindo a continuidade das operações de forma segura e resiliente.

Ao final, você deverá ser capaz de reconhecer:

- sinais de engenharia social em e-mails, SMS e outros aplicativos de mensagens, QR Codes, páginas e links falsos;
- aplicar protocolos de verificação e a separação de responsabilidades em rotinas de trabalho; e
- reportar incidentes com agilidade e segurança.

O princípio norteador de todo o aprendizado cabe em três verbos: parar, validar e reportar. Diante de algo inesperado, pare e não interaja; valide a legitimidade por um canal oficial que você já conheça; e reporte pelo canal interno de segurança sem medo de errar.

Módulo 2. Por que "Não Clique"

Capítulo 2.1 Panorama, Vetores e Riscos

A engenharia social continua entre as principais causas de violações de dados e fraudes no mundo. O Verizon Data Breach Investigations Report[1] aponta que ataques baseados em e-mail e engenharia social, como phishing e Business e-mail Compromise (BEC), permanecem entre os vetores mais frequentes e eficazes, com impacto significativo em setores como serviços financeiros, SaaS e varejo.

No Brasil, o crescimento de golpes em canais digitais, incluindo clonagem de WhatsApp, links falsos, boletos adulterados e fraudes envolvendo Pix tem crescido.

É perceptível o crescimento expressivo das fraudes eletrônicas. Segundo o levantamento do Instituto Datafolha, a pesquisa "Vitimização e Percepção da Segurança Pública no Brasil"[2] revela como os brasileiros percebem e vivenciam situações de insegurança. Um dos destaques mostra que um em cada três brasileiros sofreu um golpe na internet com prejuízo financeiro nos últimos 12 meses, o equivalente a 56 milhões de vítimas. A perda para a população com essa modalidade de crime — como golpes do Pix ou de boletos falsos, fraude contra cartão de crédito e compras não entregues — foi de R$ 111,9 bilhões.

Mas o impacto nas Corporações não se limita a perdas financeiras. Falhas de segurança exigem investigação, comunicação a clientes e autoridades, e podem gerar obrigações legais sob a égide da LGPD, além de comprometer a confiança entre a empresa e seus parceiros.

---

[1]VERIZON. 2024 Data Breach Investigations Report: Verizon, 2024. Disponível em: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[2] FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA; DATAFOLHA. Vitimização e Percepção da Segurança Pública no Brasil: 2025. São Paulo: FBSP, 2025. Pesquisa nacional realizada pelo Instituto Datafolha, encomendada pelo Fórum Brasileiro de Segurança Pública. Disponível em: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/7fa763d3-5250-4f29-a91a-6c3d6d27a7af/content

Dois mitos precisam ser quebrados logo no início:

- O primeiro: “Eu reconheço golpes facilmente.” Os atacantes personalizam abordagens com base em informação pública (como redes sociais e sites corporativos) e exploram emoções como urgência e medo, tornando enganosas até mensagens bem escritas e com logotipos legítimos.

- O segundo: “Só o pessoal de TI precisa saber disso.” Qualquer colaborador pode ser o primeiro ponto de contato de um golpista, e uma ação precipitada em qualquer área que tenha o poder de decisão de um direcionamento de pagamento a um prestador de serviços ou despesas operacionais como por exemplo: finanças, compras, atendimento ou RH, pode desencadear o redirecionamento do fluxo e gerar consequências graves para a Instituição. Segurança é responsabilidade de todos.

Capítulo 2.2 Fundamentos de Engenharia Social

A Engenharia Social é um dos vetores principais utilizado pelos criminosos para ludibriar os colaboradores internos e se materializa por um conjunto de técnicas que manipulam pessoas para que entreguem informações, executem ações fora de protocolo ou instalem softwares maliciosos.

Na prática, ela se traduz em obter “acesso a determinadas informações privilegiadas, por meio de técnicas de persuasão”[3]. Esta técnica baseia-se na exploração dos comportamentos dos indivíduos, em vez de atacar diretamente a tecnologia propriamente dita.

Ela é muito utilizada pelos criminosos que querem tirar proveito financeiro das corporações, e fazem uso de manipulação psicológica para induzir indivíduos a revelar informações confidenciais.

Os criminosos usam um conjunto de técnicas manipulativas para enganar os colaboradores internos, os prestadores de serviços terceirizados e obter acesso não autorizado a informações sensíveis. Ao invés de explorar falhas tecnológicas, os criminosos utilizam táticas de persuasão e engano para convencer as vítimas a entregar dados sensíveis, como dados bancários, senhas ou outros dados pessoais.

Ao invés de explorar falhas técnicas, explora vieses humanos:

- **A urgência** é um gatilho comum: “precisamos disso agora, caso contrário, você colocará em risco o contrato”. A autoridade é outro: “sou da área jurídica

[3] ZANIOLO, Pedro Augusto Fernando. Crimes Modernos: o impacto da tecnologia no Direito. Ed. Juspodivm. p. 248.

e o prazo para o pagamento desta guia é hoje, caso contrário perderemos a ação judicial" ou "aqui fala o diretor", frequentemente com assinatura, foto ou tom imperativo.

- **Curiosidade e reciprocidade** aparecem em mensagens como "documento importante" ou "você ganhou um brinde".

- **Medo e culpa** surgem em frases como "sua conta será bloqueada" ou "você atrasou um processo".

- **A familiaridade** fecha o cerco: o atacante utiliza nomes de colegas, clientes ou fornecedores obtidos de e-mails vazados ou redes sociais.

O ciclo de um ataque típico começa com reconhecimento, muitas vezes usando informações abertas (OSINT - Open Source Intelligence[4]), segue com a abordagem por e-mail, telefone ou mensageria, passa à exploração quando a vítima clica, fornece credenciais ou aprova um pagamento, e prossegue para a pós-exploração, quando o invasor movimenta-se dentro do ambiente, coleta dados e tenta expandir o acesso.

Alguns sinais de alerta se repetem em diferentes canais e que devem acender o red flag do colaborador:

- remetentes ou números "quase certos";
- links encurtados ou endereços que imitam domínios reais;
- pedidos que ignoram processos formais;
- insistência em manter segredo e pressão para agir imediatamente.

Reconhecer esses padrões é o primeiro passo para interromper a cadeia do golpe.

Um programa eficaz de Cultura de Segurança para Funcionários e Prestadores de Serviço Terceirizados, deve transformar esse reconhecimento em reflexo automático: ao identificar um indício de engenharia social, o colaborador deve saber exatamente como agir — interromper a interação, validar a solicitação por canais oficiais e reportar imediatamente ao time de segurança da informação ou ao superior imediato.

Mais do que memorizar exemplos, é essencial criar o hábito de questionar, confirmar e seguir protocolos, pois a verdadeira barreira contra ataques não está apenas nas ferramentas tecnológicas, mas na postura vigilante e proativa das pessoas que as utilizam.

[4] É o trabalho de coletar informações que já estão disponíveis publicamente — na internet, jornais, redes sociais, registros públicos — e usar essas informações para montar um "quebra-cabeça" sobre uma pessoa, empresa ou situação. É como fazer uma investigação usando só "pistas abertas", sem precisar invadir nada. Exemplo: se alguém vê seu perfil no LinkedIn, cruza com fotos no Instagram e dados que você publicou em fóruns, já está fazendo OSINT — e pode usar isso para conhecer seus hábitos, onde você trabalha, horários, gostos e até prever seu comportamento.

Módulo 3. Principais Instrumentos utilizados pelos criminosos e o uso da IA generativa

A evolução da Inteligência Artificial (IA) generativa trouxe ganhos significativos para empresas, mas também ampliou o arsenal dos criminosos. Ferramentas de IA generativa permitem criar e-mails, mensagens e documentos ultra-realistas, imitando com perfeição a linguagem e o estilo de executivos, sem erros de gramática ou sinais evidentes de fraude. Além disso, perfis falsos com fotos geradas por redes neurais e conteúdos alinhados ao setor da vítima são usados para dar credibilidade a contatos fraudulentos, facilitando golpes de phishing, spear phishing e Business Email Compromise (BEC)[5].

Outro instrumento poderoso é a clonagem de voz e a criação de deepfakes de áudio e vídeo. Com apenas alguns segundos de material público, criminosos conseguem reproduzir a voz de líderes corporativos para realizar ataques de vishing, solicitando pagamentos, dados ou aprovações. Em alguns casos, essa tecnologia é combinada a deepfakes de vídeo para reuniões virtuais, onde o impostor se apresenta visualmente como um gestor ou parceiro legítimo. Bots inteligentes também atuam em chats, WhatsApp e e-mails, conduzindo conversas prolongadas para conquistar confiança e induzir ações prejudiciais.

Para mitigar esses riscos, é essencial adotar políticas de validação por múltiplos canais, treinamentos contínuos com simulações de golpes baseados em IA e autenticação multifator (MFA) para transações e acessos críticos. Monitorar a exposição pública de executivos e limitar a divulgação de áudios e vídeos pode reduzir o material disponível para clonagem.

É importante citar que a criação de uma cultura organizacional que incentive o reporte rápido e sem punição é fundamental para que tentativas de fraude sejam interrompidas antes de se tornarem incidentes graves.

Capítulo 3.1 E-mail: O que são Phishing, Spear phishing e o Business Email Compromise?

Enquanto a Engenharia Social é uma técnica utilizada pelos fraudadores, o e-mail continua sendo o instrumento favorito de golpistas porque é onipresente e menos custoso, e as tentativas podem se dar por meio de 03 técnicas: Phishing, Spear phishing e o Business Email Compromise.

O Phishing em massa busca volume com mensagens genéricas de entrega, atualização de senha ou notificações fiscais. Ele é enviado para muitas pessoas ao mesmo tempo, tentando enganar para que elas cliquem em links falsos, baixem

[5] Veremos os conceitos destes tipos de golpes logo abaixo.

arquivos maliciosos ou entreguem dados. O criminoso não personaliza muito a mensagem — ele aposta que pelo menos alguns vão cair.

Exemplo:

➢ Você recebe um e-mail dizendo:
"Sua conta do Banco XPTO será bloqueada! Clique aqui para confirmar seus dados."

O link leva a um site falso que imita o banco, e ao colocar usuário e senha, o criminoso captura suas credenciais.

O Spear Phishing personaliza o conteúdo com nomes de projetos, executivos e fornecedores da empresa, para convencer a vítima de que se trata de uma mensagem legítima. Ele é altamente direcionado, pois o golpista pesquisa sobre a vítima para criar uma mensagem personalizada e muito mais convincente e pode envolver informações pessoais ou profissionais para ganhar credibilidade.

➢ Exemplo:
Você é gerente de compras de uma empresa. Recebe um e-mail aparentemente do seu fornecedor real:
"Oi, João, sobre o pedido #4567 que fechamos semana passada, segue em anexo a nova planilha de preços que discutimos."
O e-mail usa seu nome, o nome do fornecedor e um número de pedido real (obtidos por OSINT). E o anexo contém malware que abre acesso remoto ao computador.

Fique atento pois ferramentas de IA podem gerar PDFs, planilhas e apresentações praticamente idênticos aos da empresa, inclusive com logotipos e assinaturas digitais falsificadas.

Já o Business Email Compromise (BEC) é um golpe em que criminosos usam e-mails falsos ou contas comprometidas para se passar por alguém de confiança — como um chefe, diretor, fornecedor ou cliente — e convencer a vítima a fazer um pagamento, transferir dinheiro ou enviar informações sensíveis.

O foco não é infectar computadores com vírus, mas enganar pessoas usando autoridade, urgência e aparência legítima.

➢ Exemplo:
O golpista envia um e-mail que parece vir do diretor financeiro dizendo “faça essa transferência agora para não perdermos o contrato”, e o endereço de e-mail é quase igual ao verdadeiro ou realmente pertence ao diretor (caso a conta tenha sido invadida).

Na prática, um e-mail malicioso costuma apresentar um remetente com pequenas

alterações. Veja alguns sinais típicos para identificar um BEC:

Sinal de Alerta	O que Observar	Por que é Suspeito
Endereço de e-mail estranho ou "quase igual"	Um caractere trocado (ex.: @empresa.c0m em vez de @empresa.com) ou domínio alternativo	É a técnica de *spoofing* ou registro de domínio parecido para enganar o destinatário
Urgência fora do normal	"Preciso que faça essa transferência agora" ou "prazo se encerra hoje"	Cria pressão para que você aja sem verificar
Mudança repentina em dados de pagamento	Solicitação para transferir para uma nova conta ou banco, alegando "atualização"	Fraudes BEC geralmente pedem alteração de conta para desviar valores
Solicitação de manter segredo	"Não comente com mais ninguém, é uma negociação confidencial"	Isola a vítima e evita que ela valide a informação com outros
Tom ou formato incomum na mensagem	Erros de ortografia, assinatura diferente, excesso de formalidade ou informalidade	Indica que a pessoa por trás do e-mail não é o remetente real
Pedidos que fogem do procedimento normal	Solicitar transferência sem seguir o fluxo de aprovação habitual	Quebra de processo é uma forte bandeira vermelha
Endereço de resposta diferente	O campo "Responder para" leva a outro domínio	Pode indicar encaminhamento para conta controlada por criminosos

Dentro do contexto de uso da IA, a geração de e-mails e mensagens ultra-realistas no qual os criminosos podem usar modelos de linguagem já é uma realidade, como os usados por empresas legítimas, para criar textos convincentes, sem erros e adaptados ao perfil da vítima. Isso aumenta muito a eficácia de BEC (Business Email Compromise) e phishing direcionado.

Um e-mail "assinado" pelo CFO, com tom e vocabulário idênticos ao que ele usa, pedindo transferência de valores urgentes. A regra de ouro aqui é sempre confirmar

solicitações financeiras ou sensíveis por outro canal oficial (telefone, reunião, sistema interno) antes de qualquer ação.

O quadro abaixo mostra bem como o nível de personalização aumenta do phishing genérico para o spear phishing e BEC, e como o BEC é o mais focado em fraude financeira direta.

Tipo de Ataque	Definição	Personalização	Objetivo Principal	Exemplo	Meios Mais Comuns
Phishing	Golpe em massa que engana usuários para que cliquem em links falsos, baixem arquivos maliciosos ou entreguem dados.	Baixa — mensagem genérica enviada para muitas pessoas.	Roubo de credenciais, instalação de malware, coleta de dados pessoais.	E-mail dizendo: “Sua conta será bloqueada, clique aqui para confirmar seus dados”.	E-mail genérico, SMS (“smishing”), mensagens de redes sociais.
Spear Phishing	Phishing direcionado a uma pessoa ou grupo específico, usando informações personalizadas para parecer legítimo.	Alta — mensagem adaptada ao perfil da vítima.	Roubo de credenciais, instalação de malware, espionagem.	E-mail com seu nome, cargo e fornecedor real: “Segue a planilha atualizada que discutimos ontem” (contendo malware).	E-mail personalizado, mensagens privadas, redes sociais profissionais.

BEC (*Business Email Compromise*)	Fraude que finge ser comunicação legítima de negócio para induzir pagamentos ou mudanças em dados bancários.	Alta — muitas vezes envolve contas de e-mail reais comprometidas ou domínios falsos muito semelhantes.	Desvio de dinheiro ou bens através de ordens de pagamento falsas.	E-mail de "diretor" pedindo transferência urgente para conta "do fornecedor" (na verdade, dos criminosos).	E-mail (conta comprometida ou *spoofed*), raramente com links/anexos; foco na mensagem convincente.

Antes de interagir, é essencial repousar o cursor sobre os links para verificar o domínio completo, buscar sinais de inconsistência no idioma e conferir se o pedido faz sentido dentro do processo normal.

O juízo do leitor somente é afinado, por treinamentos como este, que aguçam o conhecimento nas técnicas utilizadas pelos criminosos para "vacinar" os indivíduos que lidam no dia-a-dia com assuntos diversos, auxiliando-os na identificação de situações que realmente são protocolos de alteração do fluxo legítimos, daqueles que, são tentativas ilegais de prejudicar financeiramente a empresa.

O comportamento esperado é simples: ao perceber sinais de risco - **não responda, não clique e não baixe anexos -** utilize o botão corporativo de reportar phishing ou encaminhe a mensagem ao canal de segurança da informação ou o superior imediato para análise.

Importante, se o e-mail envolve pagamento, alteração de dados ou credenciais, inicie você mesmo a validação por canal alternativo que já possua. Em caso de dúvida, é sempre melhor reportar um falso positivo do que ignorar algo suspeito.

Capítulo 3.2. SMS e mensageria: Smishing e golpes em Aplicativos de mensagens instantâneas

Mensagens de SMS[6] e aplicativos como WhatsApp e Telegram oferecem aos atacantes um ambiente ainda mais íntimo, onde as pessoas naturalmente respondem mais rápido.

Os golpes via SMS (smishing) frequentemente simulam empresas de entrega, bancos ou órgãos públicos, com links encurtados e avisos de "pendência urgente".

[6] Short Message Service, em português Serviço de Mensagens Curtas.

Já nos aplicativos de mensagens instantâneas como WhatsApp e Telegram, a falsificação de números e a criação de perfis com fotos e nomes conhecidos tornam as abordagens bastante convincentes. No WhatsApp, os golpes mais difundidos incluem a clonagem ou sequestro de contas a partir da engenharia social com códigos de verificação e o golpe do “novo número”, no qual alguém se passa por familiar ou colega pedindo transferências “só hoje”.

Uma variação corporativa envolve o suposto “fornecedor” que envia um “novo boleto”, um “novo número”, alegações de urgência, ou uma atualização de conta para recebimento, são os gatilhos que devem ativar o sinal de alerta do colaborador.

E atenção, robôs treinados para interagir com humanos podem conduzir conversas longas em chats corporativos, WhatsApp ou e-mails, sem levantar suspeitas, até conquistar confiança e extrair dados ou executar fraudes.

A resposta correta, nesses casos, passa por 04 boas práticas:

- não compartilhe códigos de verificação em hipótese alguma e ative a confirmação em duas etapas (MFA) no próprio aplicativo;

- trate pedidos financeiros por mensageria como não confiáveis por padrão e valide por ligação para o número oficial já conhecido e registrado no seu sistema;

- evite discutir assuntos sensíveis ou compartilhar links de acesso e arquivos por aplicativos pessoais.

- estabeleça políticas empresariais que proíbam tratar pagamentos em aplicativos pessoais ou corporativos. Peça o envio de um e-mail para formalizar o pedido e possibilitar a validação pelas áreas responsáveis.

Use os canais corporativos definidos pela política da empresa.

➢ Exemplo:
Fornecedor: “Oi, mudamos nossa conta para recebimento, pode pagar neste CNPJ?”
Funcionário responsável pelo Pagamento: Em vez de responder “ok” no aplicativo, encerre a conversa, abra o cadastro do fornecedor no sistema e mande um e-mail ou ligue para o telefone oficial que já constava lá, perguntando se houve, de fato, mudança de dados.

Se a resposta for negativa, você terá impedido uma fraude e um incidente, evitando prejuízos financeiros à Instituição.

Capítulo 3.3 Ligação Telefônica: Vishing e Engenharia Social em suporte e help desk

O Vishing é um tipo de golpe que combina engenharia social com ligações telefônicas. O nome vem de voice phishing — ou seja, phishing por voz.

Nesse ataque, o criminoso liga para a vítima fingindo ser alguém de confiança, como um funcionário do banco, suporte técnico, policial ou até um colega de trabalho. Ele usa técnicas de persuasão, urgência e autoridade para convencer a pessoa a revelar informações sigilosas (senhas, códigos, dados bancários) ou executar ações que beneficiem o golpe.

➢ Exemplo:
Um funcionário do setor financeiro de uma empresa recebe uma ligação de alguém que se apresenta como “o novo gerente de contas do banco parceiro”.
O golpista fala com segurança, menciona o nome correto da empresa, o CNPJ e até o nome do diretor financeiro — dados que ele conseguiu previamente via OSINT e redes sociais.

Durante a ligação, o falso gerente diz que há uma inconsistência na conta corporativa e que, por questões de segurança, precisa “validar o token” para evitar o bloqueio imediato do sistema de pagamentos. Ele solicita que o funcionário informe os códigos gerados pelo dispositivo ou pelo aplicativo do banco, alegando que é um procedimento de rotina.

A vítima, acreditando estar falando com um representante legítimo do banco e com medo de atrasar pagamentos importantes, fornece os códigos.

Em poucos minutos, os criminosos usam esses códigos para autorizar transferências fraudulentas, causando prejuízo financeiro significativo à empresa.

Esse método se tornou mais sofisticado com o uso de robocalls, vozes sintéticas geradas por IA e até identificação de chamada falsificada (caller ID spoofing), que faz o número aparecer como se fosse mesmo do banco ou da empresa.

Usando apenas alguns segundos de áudio público (exemplo: de uma palestra no YouTube ou entrevista), a IA pode criar uma voz idêntica à de um gestor. Essa voz é então usada para autorizar pagamentos, liberar acessos ou aprovar contratos por telefone.

O antídoto é o processo. Qualquer atendimento sensível começa com um roteiro de validação, usando dados que só o usuário legítimo saberia ou que foram combinados previamente (palavras-chave, IDs de ticket, confirmação por app corporativo).

Se a ligação foi recebida de um desconhecido, encerre cordialmente o contato e retorne pelo número oficial já cadastrado.

Nunca solicite nem aceite códigos de MFA por telefone ou chat. Códigos temporários são pessoais e intransferíveis.

- Eis um exemplo de diálogo seguro:
  "Entendo a urgência, mas para sua segurança preciso confirmar seu ticket aberto no sistema e realizar a validação pelo aplicativo de autenticação corporativo. Se preferir, vou encerrar esta ligação e retornar ao número cadastrado no seu perfil."

Se o interlocutor resiste ao procedimento, isso é um sinal adicional de alerta. Documente o contato em um ticket antes de qualquer ação e lembre-se: sem ticket, sem mudança.

Capítulo 3.4 Deepfake de vídeo e áudio

Deepfake de vídeo e áudio é uma tecnologia baseada em IA, especialmente deep learning, capaz de criar ou manipular imagens e sons de forma tão realista que parece autêntico.

No vídeo, rostos podem ser trocados (face swap), expressões faciais alteradas e até falas inventadas, mantendo sincronismo labial perfeito.

No áudio, a voz de uma pessoa pode ser clonada a partir de poucos segundos de gravação, reproduzindo entonação, sotaque e pausas.

Na esfera corporativa, o deepfake é perigoso porque pode simular líderes, clientes ou parceiros, autorizando pagamentos, divulgando informações estratégicas ou desinformando equipes.

- Exemplo real: Caso 2024 — Multinacional em Hong Kong
  Um funcionário participou de uma videoconferência em que acreditava estar com seu CFO e outros diretores. Todos eram deepfakes gerados a partir de imagens e vozes obtidas em redes sociais e vídeos institucionais. O "CFO" ordenou transferências urgentes para contas no exterior. O prejuízo foi de cerca de US$ 25 milhões[7].

[7] https://www.weforum.org/videos/arup-deepfake-fraud/

Boas práticas para prevenção:

- Autenticação multifator para transações críticas;
- Não confiar apenas em voz ou vídeo como prova de identidade;
- Confirmar ordens relevantes por um segundo canal independente (ex.: mensagem interna, ligação para número previamente validado);
- Treinamento de funcionários;
- Incluir módulos sobre deepfake em programas de treinamento, com exemplos reais e simulações;
- Ensinar a desconfiar de solicitações fora do padrão, mesmo que a fonte pareça confiável;
- Política de verificação dupla (regra dos quatro olhos);
- Nenhuma transferência ou decisão sensível deve ser executada por uma única pessoa, mesmo que a solicitação venha da alta liderança;
- Controle da exposição pública;
- Reduzir a quantidade de material audiovisual de líderes disponível publicamente, pois vídeos e áudios públicos alimentam a IA para criar deepfakes mais convincentes;
- Uso de tecnologias de detecção;
- Ferramentas especializadas podem analisar metadados, artefatos visuais e padrões acústicos para identificar manipulação;
- Monitoramento de menções à empresa para identificar disseminação de conteúdo falso.

Capítulo 3.5 Redes sociais, navegação e dispositivos

As redes sociais são ferramentas poderosas para networking, marketing e divulgação de resultados, mas também representam uma vitrine para quem busca explorar vulnerabilidades humanas.

Publicações aparentemente inofensivas, como detalhes sobre projetos em

andamento, organogramas internos, datas de férias, nomes de fornecedores ou até fotos do ambiente de trabalho, podem ser peças valiosas no quebra-cabeça de um ataque direcionado.

Criminosos utilizam essas informações para personalizar abordagens por meio dos instrumentos que vimos acima, tornando-as mais convincentes e difíceis de identificar.

Perfis falsos de “recrutadores”, “executivos de empresas parceiras” ou “representantes de fornecedores” são um recurso comum entre golpistas. Com discursos profissionais e fotos corporativas obtidas na internet, eles estabelecem contato e solicitam cópias de documentos ou até mesmo a realização de “testes técnicos” que incluem arquivos infectados com malware. Uma vez abertos, esses arquivos podem dar acesso ao computador da vítima, à rede corporativa ou a dados sensíveis da organização.

No dia a dia de navegação, é preciso atenção redobrada com os resultados patrocinados em buscadores. Essa prática maliciosa, conhecida como *malvertising*, consiste em anúncios pagos que direcionam o usuário para páginas falsas que imitam sites legítimos de suporte técnico, bancos ou fornecedores de softwares populares.

Ao inserir credenciais ou baixar um programa dessas páginas, o funcionário pode entregar, sem perceber, acesso direto ao criminoso. Para reduzir esse risco, é essencial digitar manualmente o endereço de sites críticos no navegador e, ao instalar softwares, priorizar fontes oficiais, verificando sempre a assinatura digital e a procedência do arquivo.

O cuidado com dispositivos físicos também é parte essencial da cultura de segurança. Pendrives ou discos externos de origem desconhecida são vetores frequentes de infecção por malware e devem ser evitados. Em ambientes compartilhados, como escritórios e coworkings, a prática de manter a mesa livre de documentos confidenciais e bloquear a tela do computador sempre que se afastar protege contra olhares curiosos e acesso não autorizado.

No home office, onde o controle físico e a supervisão direta são menores, a responsabilidade individual é ainda maior. Manter o roteador sempre atualizado, usar senhas fortes e exclusivas, habilitar a autenticação em dois fatores e, sempre que possível, separar dispositivos pessoais dos corporativos são medidas fundamentais para reduzir riscos. Essa separação evita que vulnerabilidades em um dispositivo doméstico comprometam dados e sistemas da empresa.

Essas práticas não são apenas formalidades técnicas ou burocráticas: elas funcionam como barreiras concretas contra as táticas de criminosos. Pequenas ações preventivas, quando aplicadas de forma consistente por todos os colaboradores, criam um ambiente mais seguro e diminuem significativamente as oportunidades para

que ataques tenham sucesso. A cultura de segurança não se constrói apenas com sistemas e firewalls, mas com a conscientização e o engajamento diário de cada funcionário.

Boas Práticas de Segurança para Funcionários e Prestadores de Serviço Terceirizados:

Redes Sociais

- Não publique detalhes sobre projetos, organogramas, férias, fornecedores ou ambiente de trabalho.
- Pense antes de postar: criminosos usam essas informações para ataques direcionados.

Contatos e Perfis Suspeitos

- Desconfie de perfis de “recrutadores” ou “executivos” que pedem currículos ou documentos.
- Nunca abra “testes técnicos” ou anexos sem verificar a origem.

Navegação Segura

- Cuidado com resultados patrocinados em buscadores (malvertising).
- Digite manualmente endereços de sites críticos (banco, sistemas corporativos).
- Baixe softwares apenas de fontes oficiais e verifique assinatura digital.

Dispositivos e Acesso Físico

- Não conecte pendrives ou discos de origem desconhecida.
- Mantenha mesa limpa de documentos confidenciais.
- Bloqueie a tela ao se ausentar.

Segurança no Home Office

- Atualize o roteador e utilize senhas fortes e exclusivas.
- Ative autenticação em dois fatores sempre que possível.
- Separe equipamentos pessoais dos corporativos.

Princípio Geral

- Pequenas ações diárias fortalecem a segurança da empresa.
- Se algo parecer estranho, não clique e reporte ao time de segurança

Módulo 4. Como prevenir Fraudes e Golpes

Capítulo 4.1 Protocolos e separação de responsabilidades

A separação de funções (SoD, do inglês Separation of Duties) estabelece que atividades críticas não devem ser iniciadas, aprovadas e executadas por uma única

pessoa. Segregar Funções é uma das estratégias mais eficazes para prevenir que a Instituição seja vítima de um golpe bem-sucedido pois impede que uma única pessoa tenha controle total sobre um processo financeiro ou administrativo, reduzindo as oportunidades para fraudes.

Principalmente em áreas responsáveis por pagamentos, ou que tenham acesso a valores monetários, por exemplo, quem cria a ordem não deve ser o mesmo que aprova a transferência.

Ações Recomendadas:

- Segregação de funções: Distribuir responsabilidades entre diferentes pessoas para processos-chave, como aprovação de pagamentos, lançamentos contábeis e auditorias internas.

- Controle de acessos e permissões: Limitar o acesso a informações sensíveis de acordo com a necessidade de cada função, utilizando sistemas de gestão de identidades e acessos.

- Auditorias periódicas e revisões: Realizar auditorias internas frequentes e revisões regulares dos processos financeiros e administrativos para identificar comportamentos irregulares.

O princípio do menor privilégio complementa a proteção, garantindo que cada colaborador tenha acesso apenas ao necessário para suas funções.

Uma camada prática crucial é a verificação por canal independente. Se um e-mail pede a mudança de conta bancária de um fornecedor, a confirmação deve ocorrer por ligação para o número oficial já registrado no cadastro, e não para o telefone informado no próprio e-mail.

Em serviços que oferecem suporte técnico e assistência a usuários - *help desk* -, redefinições de senha ou desbloqueios sensíveis exigem validações com dados previamente combinados e, quando possível, confirmação multifator.

Exceções por “urgência do diretor” sem registro e aprovação formais são um vetor clássico de engenharia social.

A cultura correta é:
- sem ticket, sem ação;
- sem validação independente, sem mudança;
- sem os “quatro olhos”, sem pagamento.

Estas boas práticas, presentes em normas internacionais como a do National Institute

of Standards and Technology - NIST SP 800-53[8], e do International Electrotechnical Commission - ISO/IEC 27001[9] -, reduzem significativamente o risco de fraude, e devem ser obtidas por Instituições que querem obter uma Certificação com o escopo de mitigar riscos.

- NIST SP 800-53: É uma publicação do National Institute of Standards and Technology (NIST), dos Estados Unidos, e serve como referência global para práticas de segurança robustas. Lista um conjunto muito detalhado de controles de segurança e privacidade que organizações podem implementar para proteger sistemas de informação federais e dados sensíveis. No site eles trazem um modelo de Índice de Colaboração de Controle de Segurança e Privacidade, que é organizado por famílias de controles, como controle de acesso, resposta a incidentes, continuidade de negócios, segurança física, criptografia, entre outros.

- ISO/IEC 27001: É uma norma internacional que define os requisitos para implementar um Sistema de Gestão de Segurança da Informação (SGSI). Foca menos em uma lista extensa de controles técnicos e mais em processos e governança, para que a organização crie, mantenha e melhore continuamente sua postura de segurança. Tem como foco o ciclo de melhoria contínua (PDCA) e alinhamento da segurança com os objetivos do negócio. É certificável — ou seja, empresas podem obter um certificado ISO/IEC 27001 após auditoria externa, o que muitas vezes é exigido em contratos e licitações.

Mas se uma empresa não precisa obter um certificado, adotar os protocolos que trazemos aqui, com procedimentos simples e bem comunicados, bloqueia boa parte das tentativas de golpe. O importante é o aculturamento de todos aqueles que fazem parte da cadeia operacional e financeira, ainda que não diretamente, de uma Companhia, não importa o seu porte, grande, média, pequena ou micro empresa.

Capítulo 4.2. Programa contínuo de conscientização

A conscientização em segurança cibernética não deve ser tratada como um evento isolado ou uma palestra anual, mas sim como um **programa contínuo e vivo**, capaz de evoluir junto com as ameaças e com a própria cultura organizacional.

O envolvimento e o patrocínio visível da liderança são fatores determinantes para o sucesso, transmitindo não apenas a prioridade do tema, mas também a mensagem de "denúncia sem culpa", incentivando os colaboradores a reportarem situações suspeitas sem receio de represálias.

[8] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (Security and Privacy Controls for Information Systems and Organizations)
[9] https://www.iso.org/standard/27001 (International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC)

Treinamentos curtos, frequentes e dinâmicos tendem a ter maior eficácia do que longas sessões anuais que se tornam rapidamente obsoletas. A aplicação de simulações realistas — como campanhas de phishing, vishing e smishing — seguida de feedback individual e coletivo, transforma o aprendizado em reflexos automáticos. Isso reduz o tempo de reação diante de uma tentativa real e fortalece a postura preventiva.

Áreas críticas, como financeiro, compras e TI, demandam treinamentos sob medida, alinhados aos riscos e processos específicos do setor. Isso inclui práticas como a **validação de dados bancários por canais independentes**, aplicação rigorosa da **"regra dos quatro olhos"** em aprovações sensíveis e uso consistente de autenticação multifator. Além disso, a criação de **embaixadores de segurança** em cada área amplia a capilaridade do tema, promovendo a troca de informações e acelerando a identificação de vulnerabilidades internas.

A mensuração de resultados é essencial para evoluir o programa. Indicadores como redução da taxa de clique em simulações, aumento da taxa de reporte, tempo médio entre a detecção e o reporte, grau de adesão à separação de funções, cobertura de MFA e número de tentativas de BEC detectadas fornecem dados concretos para priorizar ações.

Por fim, incidentes reais devem sempre ser seguidos de análises construtivas e sem caça às bruxas, com atualização imediata de treinamentos e playbooks - guia prático que descreve, passo a passo, o que fazer, quem acionar e como agir -, fechando o ciclo da melhoria contínua e consolidando a Cultura de Segurança no DNA da organização.

Módulo 5. Reporte e resposta a incidentes

Capítulo 5.1 Saber reportar é tão importante quanto saber reconhecer.

Saber reportar um incidente é tão importante quanto saber reconhecer um golpe. Identificar uma ameaça é apenas a primeira etapa; a resposta rápida e correta é o que realmente reduz danos e impede que um problema isolado se torne uma crise generalizada.

Clique acidental em link suspeito, inserção de credenciais em site duvidoso, recebimento de ligação enganosa, perda ou roubo de dispositivo e instruções de pagamento fora do processo são situações que exigem notificação imediata.

Para isso, a empresa deve ter um **Protocolo de Resposta a Incidentes** claro e conhecido por todos os colaboradores:

1. Identifique o incidente

• Clique acidental, inserção de credenciais, ligação suspeita, perda de dispositivo

ou solicitação de pagamento fora do processo.

2. Reporte imediatamente
• Encaminhe e-mails suspeitos via 'reportar phishing' ou como anexo intacto.
• Registre números, horários, prints e conteúdo de mensagens ou ligações.

3. Preserve evidências
• Não apague dados.
• Não tente investigar diretamente o atacante.

4. Ação das equipes internas
• TI: isolar máquinas, redefinir credenciais, analisar logs.
• Jurídico/Privacidade: avaliar obrigações legais.
• Comunicação: preparar mensagens internas e externas.

O tempo é crítico: agir nos primeiros minutos pode evitar violações maiores.

Após o reporte, as equipes técnicas agirão para isolar máquinas, redefinir credenciais e analisar logs. O departamento jurídico e a área de privacidade avaliarão possíveis obrigações legais e notificações regulatórias. Já a área de comunicação ficará responsável por elaborar mensagens internas e externas, garantindo que a informação seja tratada com precisão e sem gerar pânico.

O tempo de resposta é fator crítico: ações tomadas nos primeiros minutos podem impedir que um acesso indevido evolua para uma violação de dados em larga escala. Em segurança cibernética, a velocidade e a precisão no reporte salvam não apenas sistemas e informações, mas também a reputação da empresa.

Módulo 6. Estudo de Caso Real

No início de 2024, fraudadores deram um prejuízo US$ 25 milhões na empresa Arup. Eles usaram uma versão clonada digitalmente de um gerente sênior, sediado em Hong Kong, para enganar um funcionário e fazê-lo realizar transferências financeiras[10].

O golpe começou com uma fase minuciosa de reconhecimento: os criminosos mapearam executivos, fluxos de pagamento e relacionamentos da empresa usando fontes públicas (OSINT), como redes sociais, comunicados de imprensa e documentos corporativos.

Posteriormente fez com que o trabalhador fosse levado a participar de uma reunião

[10] Disponível em: https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-golpista-que-usou-deepfake-para-simular-reuniao/#goog_rewarded e Veja vídeo do CIO da Arup: https://www.weforum.org/videos/arup-deepfake-fraud/

virtual, com a presença do CEO e outros membros da equipe, mas todos na verdade eram criações falsas.

A tecnologia utilizada reproduziu não apenas a imagem do executivo, mas também suas expressões faciais e entonação vocal, fazendo com que os funcionários acreditassem que a solicitação era legítima. O ataque resultou em uma fraude de cerca de 25 milhões de dólares.

Inicialmente, o funcionário suspeitou que se tratasse de um e-mail de phishing, pois falava da necessidade da realização de uma transação secreta. No entanto, ele deixou de lado as suas primeiras dúvidas após a video chamada porque outras pessoas presentes pareciam e soavam como colegas que ele reconhecia.

O golpe só foi descoberto quando o funcionário posteriormente consultou a sede da corporação, no Reino Unido.

Segundo o Diretor Global de Informações da Arup, não se tratou de um ataque cibernético no sentido usual, pois nenhum sistema foi comprometido. Um termo mais adequado seria "engenharia social aprimorada pela tecnologia".

Tecnologias e Engenharia Social Envolvidas:

- **Deepfake de vídeo** para reuniões virtuais, replicando aparência e gestos.
- **Clonagem de voz** para reforçar credibilidade nas solicitações.
- **Engenharia social** explorando gatilhos de urgência e autoridade.
- Possível uso de *phishing* prévio para capturar dados internos, como agendas e padrões de comunicação.

Ações Recomendadas e Boas Práticas

1. **Validação por múltiplos canais**: confirmar solicitações financeiras ou de dados sensíveis por telefone ou presencialmente, com um canal previamente acordado.
2. **Treinamento contínuo**: incluir simulações de golpes com deepfake, *vishing* e *BEC* nos programas de conscientização.
3. **Redução da exposição pública**: evitar a publicação excessiva de vídeos e áudios de executivos em canais abertos.
4. **Autenticação multifator (MFA)** em sistemas financeiros e de aprovação.
5. **Política de "regra dos quatro olhos"**: nenhuma transação crítica deve ser

aprovada por apenas uma pessoa.

Módulo 7. Conclusão

A pandemia de Covid-19 acelerou mudanças profundas no ambiente corporativo, abrindo espaço para modelos de trabalho remoto e híbrido que permanecem até hoje. Embora esses formatos tragam benefícios como flexibilidade e redução de custos, eles também trouxeram novos desafios para a segurança da informação. A ausência da interação presencial e a dependência maior de canais digitais alteraram a forma como equipes se comunicam e validam solicitações internas.

Essa nova dinâmica compromete, em muitos casos, a capacidade de identificar solicitações suspeitas ou de confirmar informações diretamente com colegas e gestores. Essa fragilidade de comunicação e validação abre oportunidades para criminosos explorarem lacunas nos processos e aplicarem golpes cada vez mais sofisticados, principalmente por meio de engenharia social, phishing e ataques direcionados.

Diante desse cenário, o desafio das empresas vai além do investimento em soluções tecnológicas. É necessário criar e manter uma cultura de segurança cibernética que envolva todos os colaboradores, transformando cada funcionário em um agente ativo de prevenção. Isso significa ensinar a identificar riscos, reconhecer sinais de fraude e saber agir diante de situações suspeitas, seja no escritório ou trabalhando de casa.

Treinamentos como o programa “Não Clique” são fundamentais para atingir esse objetivo. Ao capacitar continuamente os funcionários, a empresa não apenas reduz a probabilidade de incidentes, mas também fortalece a resiliência organizacional. A prevenção precisa se tornar parte da rotina, com atenção, questionamento e uso rigoroso de protocolos, garantindo que a segurança digital esteja incorporada à cultura corporativa.

Transformar teoria em prática depende de algumas decisões simples e repetidas. Diante de um e-mail inesperado com tom urgente, lembre-se:

> “A rapidez é amiga do golpista, não sua.”

A cultura que queremos é aquela em que o colaborador que pergunta não é visto como chato, mas como alguém responsável.

Adapte exemplos e processos à realidade da sua organização, registre e socialize exceções. Golpes evoluem com rapidez e, mais do que decorar sinais, é preciso cultivar o hábito de **pausar, validar e reportar** até que se torne automático. Quando todos jogam com o mesmo manual, a organização inteira fica mais fortalecida e menos suscetível a vulnerabilidades.

Módulo 8. Referências Bibliográficas

CNN BRASIL. Funcionário de multinacional paga US$ 25 mi a golpista que usou deepfake para simular reunião. Disponível em: https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-golpista-que-usou-deepfake-para-simular-reuniao/. Acesso em: 20 ago. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA; DATAFOLHA. Vitimização e Percepção da Segurança Pública no Brasil: 2025. São Paulo: FBSP, 2025. Pesquisa nacional realizada pelo Instituto Datafolha. Disponível em: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/7fa763d3-5250-4f29-a91a-6c3d6d27a7af/content. Acesso em: 20 ago. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). ISO/IEC 27001 – Information Security Management Systems. Disponível em: https://www.iso.org/standard/27001. Acesso em: 20 ago. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. Disponível em: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Acesso em: 20 ago. 2025.

VERIZON. Data Breach Investigations Report 2024. [S.l.]: Verizon, 2024. Disponível em: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Acesso em: 20 ago. 2025.

YOUTUBE. Funcionário de multinacional paga US$ 25 mi a golpista que usou deepfake para simular reunião. Disponível em: https://www.youtube.com/watch?v=o1J9iNgVSvI. Acesso em: 20 ago. 2025.

ZANIOLO, Pedro Augusto Fernando. Crimes Modernos: o impacto da tecnologia no Direito. São Paulo: Juspodivm, p. 248.