



Material de conscientização sobre fraudes na internet.

Com intuito de promover uma maior conscientização no uso seguro de recursos tecnológicos, a equipe da Unidade de Segurança da Informação e Comunicação, junto a Diretoria de Tecnologia da informação disponibilizará materiais de recomendação e boas práticas.

Este material é uma reprodução da cartilha disponibilizada pelo [CERT.BR](https://www.cert.br).

Phishing

*Phishing*², *phishing-scam* ou *phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;
- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento, como exemplificado na Tabela 2.1³. Exemplos de situações envolvendo *phishing* são:

Páginas falsas de comércio eletrônico ou *Internet Banking*: você recebe um *e-mail*, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um *link*. Ao fazer isto, você é direcionado para uma página *Web* falsa, semelhante ao *site* que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

Páginas falsas de redes sociais ou de companhias aéreas: você recebe uma mensagem contendo um *link* para o *site* da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página *Web* falsa onde é solicitado o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas que passarão a ter acesso ao *site* e poderão efetuar ações em seu nome, como enviar mensagens ou emitir passagens aéreas.

Mensagens contendo formulários: você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

Mensagens contendo *links* para códigos maliciosos: você recebe um *e-mail* que tenta induzi-lo a clicar em um *link*, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você abri-lo/executá-lo, será instalado um código malicioso em seu computador.

Solicitação de recadastramento: você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de *e-mail* está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, <i>Voxcards</i> , Yahoo! Cartões, O Carteiro, <i>Emotioncard</i>
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em <i>site</i> de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
<i>Internet Banking</i>	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
<i>Reality shows</i>	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama <i>online</i>
Serviços de <i>e-mail</i>	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
<i>Sites</i> com dicas de segurança	aviso de conta de <i>e-mail</i> sendo usada para envio de <i>spam</i> (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Prevenção:

- fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;
- questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
- não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada (mais detalhes na Seção **3.3** do Capítulo **Ataques na Internet**);
- seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;
- verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing*. Ao posicionar o *mouse* sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing* (mais detalhes no Capítulo **Mecanismos de segurança**);
- verifique se a página utiliza conexão segura. *Sites* de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados (mais detalhes na Seção **10.1.1** do Capítulo **Uso seguro da Internet**);
- verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro (mais detalhes na Seção **10.1.2** do Capítulo **Uso seguro da Internet**);
- acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

Referencias: <https://cartilha.cert.br/golpes/>