

ENGENHARIA SOCIAL

Método de **ataque**, onde alguém faz uso da **persuasão**, muitas vezes abusando da ingenuidade ou confiança do usuário, para **obter informações** que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.



ENGENHARIA SOCIAL: EXEMPLOS

- E-mail do suporte técnico do banco dizendo que o arquivo em anexo resolve um problema de segurança do *home banking*.
- E-mail dizendo que o computador está infectado por um vírus que só pode ser removido através da instalação de uma ferramenta disponível no link.
- Ligação de telefone dizendo ser o provedor da internet e informando que precisa da senha para corrigir um problema na conexão;
- Ligação de telefone informando ter sequestrado um parente próximo e pedindo que o resgate seja depositado em poucas horas;
- Salas de bate-papo para atrair crianças.



COMO SE PROTEGER?

- Bom senso é essencial.
- Solicitações de informações pessoais e senhas por telefone, e-mail, etc.
- Não tentar acessar links que chegam por e-mail antes de consultar as instituições que dizem ser as responsáveis pela mensagem.



KEVIN MITNICK

- Durante os anos 70, quando invadiu o computador da sua escola e alterou algumas notas.
- Invadiu vários computadores, como de operadora de celulares, de empresas de tecnologia e provedores de internet.
- Foi preso em 1995 e libertado em 2000 após pagar uma fiança de U\$64000.



KEVIN MITNICK

- Após cinco anos preso, Kevin Mitnick foi libertado com a condição de manter-se longe de computadores, celulares e telefones portáteis pelo período de três anos.
- Em 1994, Tsutomu Shimomura era um grande especialista em segurança do Centro Nacional de Supercomputação em San Diego, Califórnia. Teve o computador invadido por Kevin. Para não deixar sua imagem manchada ajudou o FBI a encontrar Kevin.



KEVIN MITNICK

- Atualmente Kevin Mitnick escreve livros e artigos sobre segurança de informações, profere palestras em diversos países e trabalha como consultor em segurança de sistemas.
- <http://mitnicksecurity.com/>
- História já rendeu 3 livros:
 - "TAKEDOWN",
 - "O PIRATA E O SAMURAI"
 - "JOGO DO FUGITIVO".



SCAM (“GOLPE”)

É qualquer **esquema ou ação enganosa** e/ou **fraudulenta** que, normalmente, tem como finalidade obter vantagens financeiras.



SCAM (“GOLPE”)

- Realizados através de páginas WEB
 - **Exemplo:** Sites de leilões e de produtos com preços “muito atrativos”. Ao efetivar a compra, na melhor das hipóteses, receberá um produto que não condiz com o solicitado.
- Através do recebimentos de e-mail
 - **Exemplo:** Recebe um e-mail de uma instituição governamental onde é solicitado que você atue como intermediário numa transferência internacional de fundos (*Nigerian 4-1-9 Scam*)



PHISHING OU PHISHING / SCAM

Fraude que se dá através do envio de **mensagem** não solicitada, que se passa por comunicação de uma **instituição conhecida**, que procura induzir o acesso a **páginas fraudulentas** (falsificadas).




PHISHING OU PHISHING / SCAM


- Phishing vem da analogia com “fishing”. Iscas usadas para pescar senhas e dados financeiros.
- Mensagem que procura induzir a instalação de códigos maliciosos.
- Mensagem que apresentam no próprio conteúdo formulários para enviar dados.
- Comprometimento do serviço DNS.



COMO SE PROTEGER?

- Realizar transações apenas em sites de instituições confiáveis.
 - Procurar sempre digitar no browser o endereço desejado.
 - Certifica-se que o endereço apresentado no browser corresponde ao site que você deseja visitar.
 - Certifica-se que o site faz uso de conexão segura.
- 

COMO SE PROTEGER?

- Antes de aceitar um certificado, verificar junto à instituição que mantém o site sobre sua emissão e os dados neles contidos.
 - Desligar sua Webcam antes de acessar um site de comércio eletrônico ou internet banking.
 - Atenção aos ataques de engenharia social.
- 

CUIDADOS ADICIONAIS...

- Manter o browser sempre atualizado e com todas as correções aplicadas.
- Restringir execuções de JavaScript, Java e ActiveX sem permissão.
- Bloquear pop-up no browser.
- Configurar leitor de e-mail para não abrir arquivos ou executá-los automaticamente.
- Não executar programas obtidos pela internet ou e-mail.



ALGUNS PHISHING / SCAM 2010



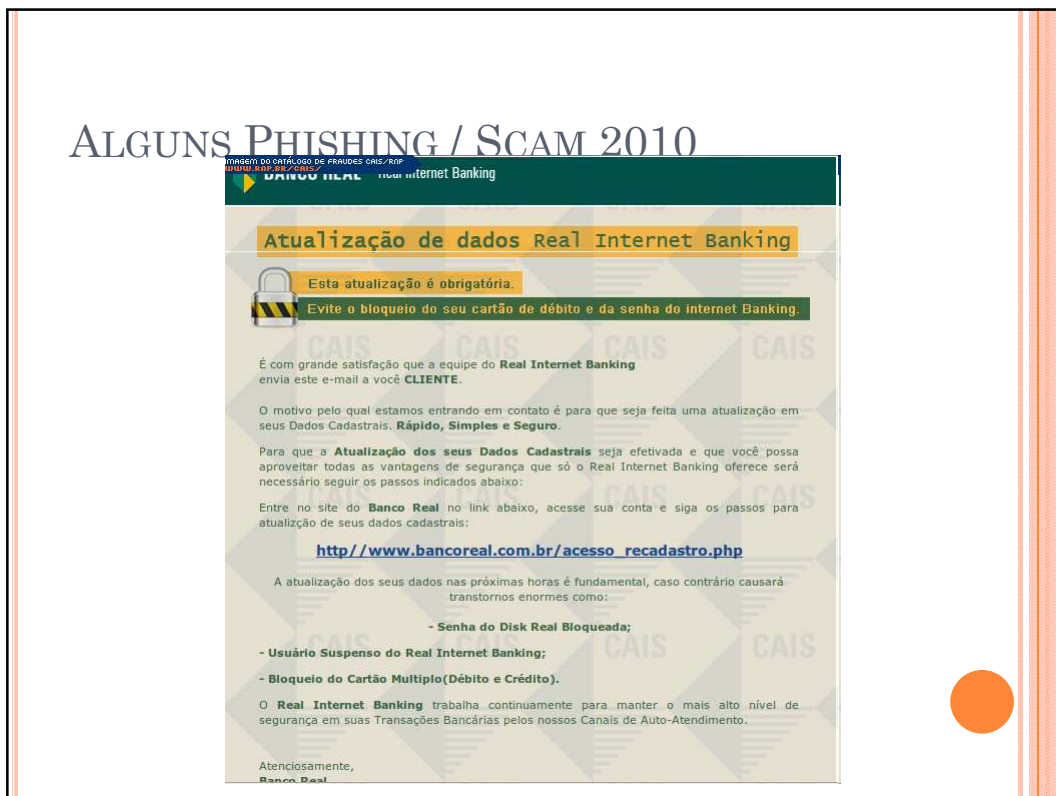
ATENÇÃO: NÃO RESPONDA ESTE E-MAIL. TRATA-SE DE UMA MENSAGEM AUTOMÁTICA. LEIA O PASSO A PASSO PARA PARTICIPAR E TROCAR SEUS PONTOS POR PRODUTOS E SERVIÇOS.

PASSO 1. CADASTRE-SE AQUI

PASSO 2. CONHEÇA OS PARCEIROS DO PROGRAMA SURPREENDA. VOCÊ PODE TROCAR SEUS PONTOS POR VÁRIOS PRODUTOS E SERVIÇOS. CONHEÇA OS PARCEIROS E VEJA O NÚMERO DE PONTOS NECESSÁRIOS PARA A TROCA DE CADA UM. QUANTO MAIS USAR SEU CARTÃO DE CRÉDITO OU DÉBITO MASTERCARD, MAIS PONTOS VOCÊ GANHA.

PASSO 3. TROQUE SEUS PONTOS: ESCOLHA O PARCEIRO E COMPRE UM PRODUTO OU SERVIÇO QUE VOCÊ DESEJA. TROQUE OS PONTOS QUE VOCÊ ACUMULOU NO PROGRAMA POR OUTRO PRODUTO OU SERVIÇO. VOCÊ RECEBERÁ UM VOUCHER, QUE DEVERÁ SER IMPRESSO E TROCADO PELO BENEFÍCIO.

ALGUNS PHISHING / SCAM 2010



ALGUNS PHISHING / SCAM 2010

IMAGEM DO CATÁLOGO DE FRADES CHIS/RIP
www.correios.com.br/CAIS/

Caso esteja vendo as imagens abaixo acinzentadas clique acima em "Mostrar conteúdo"

ALGUNS PHISHING / SCAM 2010

IMAGEM DO CATÁLOGO DE FRADES CHIS/RIP
www.visa-br.com/CAIS/

Parabéns! Seu pedido foi concluído com sucesso e neste momento, encaminhado para o faturamento. Assim que recebermos autorização da sua administradora de cartão de crédito, o mesmo será expedido.

VISA-Brasil @ www.visa-NET.com.br/Extrato-Compras.

Nº do seu pedido: 11226133

Nome do produto:	Quantidade:	VALOR:
TV LCD 32" - Conversor Digital Integrado, Full HD, 2 HDMI, USB - 32PFL3605D - PHILIPS (Ref: 49205) - ST	1	R\$ 1.799,00
Camisa Copa Mastercard (Ref: 1075) - ST	1	Brinde

Forma de pagamento:

Cartão de Crédito	Desconto: R\$ 0,00
Cartão MasterCard Qtd parcelas: 4 no valor de R\$ 449,75	Valor do frete: GRÁTIS
	TOTAL: R\$ 1.799,00

Sociedade Comercial e Importadora Hermes S.A.
 Av. Brasil 44.228, Rio de Janeiro, RJ - CNPJ 33.068.883/0002-01 - Inscrição Estadual 82.367.179

ALGUNS PHISHING / SCAM 2010

IMAGEM DO CATALOGO DE FRAUDES CRIS/RAP
R0100_R01P_RR/CRIS/



MasterCard® e TAM Viagens - Paga 1, Viajam 2

Para este benefício você precisa de **15 pontos**.

Faça a viagem dos seus sonhos ao lado de alguém especial.

+ 15 = PONTOS

Clientes MasterCard® agora tem muito mais benefícios com o Programa Surpreenda. Com 15 pontos apenas, você compra um pacote de viagens e leva 2.

Basta se cadastrar e usar seu cartão. A cada R\$ 50,00 gastos, você ganha 1 ponto para trocar em produtos ou serviços de nossos parceiros. Além de concorrer a prêmios em dinheiro.

Confira os destinos e boa viagem.


CLIQUE AQUI E CADASTRE-SE

Todos os produtos do Programa Surpreenda estão sujeitos à disponibilidade de estoque. Fotos meramente ilustrativas, devendo apenas servir de exemplo quanto aos gêneros dos produtos ofertados pela TAM Viagens.


BOATOS (HOAXES)

São **e-mails** que possuem **conteúdos alarmantes ou falsos** e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental.


QUAIS OS PROBLEMAS?

- O objetivo do criador do boato normalmente é saber por quanto tempo ele vai ficar se propagando.
 - Mas também podem conter códigos maliciosos.
 - Podem ser usados como ferramenta para engenharia social.
 - Podem comprometer imagem da instituição.
- 

COMO EVITAR OS BOATOS?

- Checar a precedência do e-mail
 - Mesmo sendo de alguém conhecido é interessante certifica-se:
 - <http://www.quatrocantos.com/LENDAS/>
 - <http://www.desaparecidos.mj.gov.br/>
 - <http://urbanlegends.about.com/>
 - <http://www.snopes.com/>
- 

ALGUNS BOATOS...

- Dilma Rousseff condenada nos Estados Unidos? (2010)
 - Batom com chumbo dá câncer (2009)
 - Orkut e MSN serão pagos (2009)
 - Turista no World Trade Center em 11/09/2001
 - Criança doente precisa de sua ajuda (1989)
 - Bill Gates distribui dinheiro (1997)
 - Imposto de cinco centavos por e-mail (1999)
- 

REFERÊNCIAS

- Cartilha de segurança para Internet. Versão 3.1. Comitê Gestor da Internet no Brasil.
 - <http://www.fraudes.org>
 - <http://www.cert.br/>
 - <http://www.rnp.br/cais/fraudes.php>
 - http://veja.abril.com.br/entrevistas/kevin_mitnick.shtml
- 