

Phishing Scam

A fraude do Século XXI

Por: Diego de Oliveira Martins



Grupo de Resposta a Incidentes de Segurança

Departamento de Ciência da Computação

Instituto de Matemática

Universidade Federal do Rio de Janeiro – Brasil



Crimes Virtuais

Mundo Contemporâneo: Virtualização de ações rotineiras

Criminosos também acompanham tendências.

Fatores que favorecem:

- Alto nível de ocultação;
- Ausência de legislação específica;
- Capacidade de discernimento reduzida;
- Passa a valer o grau de instrução;



O que é Phishing Scam?

Origem: Do inglês *Fishing* – Pescaria (senhas);

Citado pela primeira vez em 1996;

Emprega mensagens em geral e sites falsos.

Danos causados:

- Perda de dados sensíveis;
- Prejuízos financeiros, muitas vezes exorbitantes;

Índice de sucesso superior a 5% (APWG).



Phishing e Engenharia Social

Soluções de SI tornam a vida de indivíduos maliciosos mais difícil.

Necessidade do uso de um método eficaz.

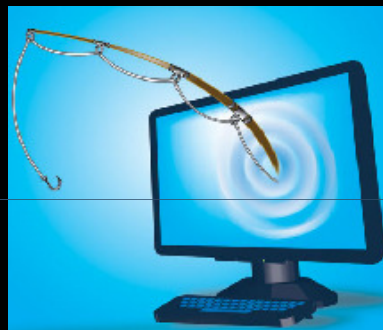
Assimilação do conceito de Engenharia Social na área de SI.

Ataque conduzido a nível psicológico → Não há softwares de proteção.

Ataques de Phishing Scam baseiam-se largamente em E.Social (Confiabilidade)



Vertentes do Phishing



Diversas vertentes:

- Spear Phishing
- Fraude 419
- iPhishing
- Vishing Scam
- Phishing em Mensageiros Instantâneos
- Phishing em Sites de Relacionamento



Spear Phishing



Ataques de Phishing altamente focalizados

Correlacionando ao nome Phishing, corresponde a “Pesca com arpão”.

Mais demorado: Exige longa e minuciosa etapa de pesquisa, além de paciência.



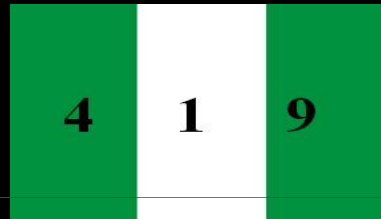
Spear Phishing

O ataque:

- Definição do alvo;
- Sondagem de informações em nível crescente de importância.
- Possuindo informação suficiente, passa-se por alguém de poder.
- Elaboração de e-mail de estrutura similar aos que circulam internamente,
- Apresenta a solicitação de dados sensíveis, ou download de malwares.
- Obtém acesso a informações sigilosas e pode realizar, por exemplo, transferências (no caso de bancos).



Fraude 419



Criada na década de 80 (crise petrolífera da Nigéria);

Origem do termo: Seção 419 do Código Penal Nigeriano(“171” brasileiro).

Popularização do uso do e-mail → Fraude mais barata, mais eficaz (SPAM).

É um verdadeiro jogo.

Riscos e regras obscuras a cargo do time de atacantes.



Fraude 419

O ataque:

- Assimilação de identidade (Alto funcionário – BC Nigeriano, etc)
- E-mail solicitando à vítima permissão para utilizar sua conta bancária
- Motivo: Efetuar grandes transferências (da ordem de milhões)
- Justificativas: Evitar taxas, desvio discreto de dinheiro, investimentos.
- Motivação inicial: Ganância.
- Ludibriação: Criação de situação que sugira máximo de segurança à vítima



Fraude 419

- Em caso de interesse da vítima, inicia-se o jogo:
- Troca de fotos e informações pessoais;
- Estabelecimento de laços mais fortes;
- Envio de documentos (apenas) aparentemente legítimos.
- Atacante sugere existência de obstáculos
- Solicitação de dinheiro para cobrir despesas imediatas (subornos, etc).
- Motivação intermediária: Laços de confiança, medo de fracasso no negócio.
- Solicitação de outros pagamentos.
- Motivação final: Medo de perder o dinheiro investido anteriormente.



Fraude 419

O lado obscuro do jogo:

- A vítima é convidada a viajar para a Nigéria.
- Atacante sugere que não solicite visto (discrição).
- Contra-ponto: Amigos resolverão eventuais problemas.
- Sem passaporte, ilegalidade → Mais vulnerável.
- Levada para cativeiro.
- Desaparecimento ou óbito.

- Famílias arruinadas, financeira e/ou socialmente.



iPhishing



Contexto atual: Disseminação da internet e rápida evolução tecnológica

Onda de modernidade: Design e funcionalidade, segurança em 2º plano.

Exemplo:

Portabilidade - Limitações de espaço físico (tela e dispositivos de entrada)

Falha de segurança - Ocultação de URL e navegação por links.

Vertente que visa explorar vulnerabilidades conseqüentes do avanço excessivamente rápido da tecnologia.



iPhishing

O ataque:

- Pode ocorrer de diversas maneiras. Exemplo: Envenenamento de DNS.
- Ocultação de URL em portáteis (parcial ou total) → Impossível checar legitimidade.
- Maior propensão a cair em golpes de Phishing.
- Pode-se explorar outras vulnerabilidades. Exemplo: Método scrollto().
- Faz-se com que a página salte para onde não se possa ver a URL original.
- Ao aproximar-se do topo (URL), salta-se para outro ponto da página.

Grande campo para Phishers.



Vishing Scam



Inventividade humana: Buscar uso maléfico para novas tecnologias.

Utiliza-se da tecnologia VoIP (Voice over IP)

- Tecnologia de baixo custo: Ataques baratos e eficazes.
- Possibilidade de mascarar o número a ser identificado pelo receptor: Ocultação e disfarce.



Vishing Scam

O ataque:

- Envio de mensagens para o celular da vítima, na tentativa de conduzi-la a discar para um número fornecido. Justificativas variam. Exemplo: Banco.
- Caso a vítima disque, é atendida por um sistema eletrônico de voz, criada para simular a de alguns bancos.
- Solicitação de inserção de dados da conta no teclado do aparelho, como conta bancária e senha de acesso.
- A voz declara a reativação da conta. Porém, a vítima acaba de ser fisgada.
- Atacante acaba de ter acesso a dados sensíveis.



Vishing Scam

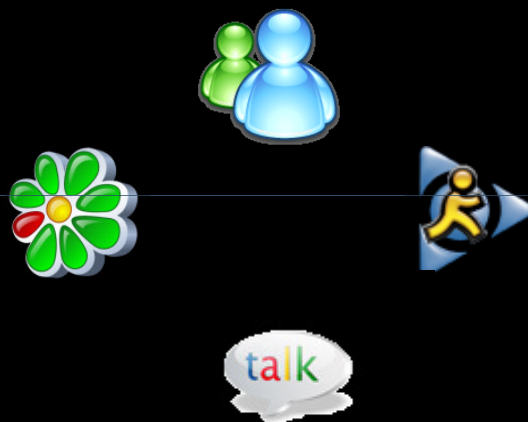
Outras possibilidades:

Há formas “agressivas” de realizar o ataque.

- *Spoof* do número de origem.
- Uso de scripts para iniciar chamadas VoIP (faixa de números).
- Ao encontrar caixa de mensagens, deixa-se solicitação de contatar número dado.
- É um SPIT (Spam Over Internet Telephony).
- Pouco difundido no Brasil, mas nos atingirá num futuro breve.



Phishing em Mensageiros Instantâneos



Terreno bastante fértil.

Motivos:

- Tipo de comunicação;
- Ambiente “descontraído”;
- Troca frequente de URL's;
- Grau de conhecimento dos usuários (maioria);



Phishing em sites de relacionamento



Por motivos similares aos M.I., são terrenos férteis.

Motivos (Além do explicitado anteriormente):

- Rede onde circulam informações da vida alheia e fotografias.
- A menos que seja definida como privada, a página de recados é de acesso público;
- Devido a desenfreada inclusão digital, presença de muitos usuários leigos.



A condução de um ataque tradicional

São 6 as fases que compõem um ataque tradicional:

Fase de Planejamento (Fase inicial)

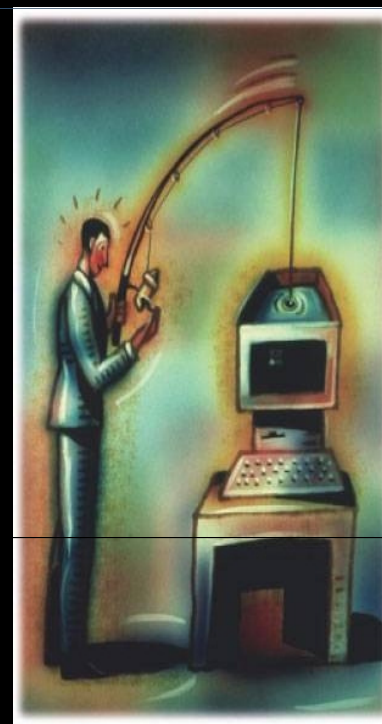
Fase de Preparação

Fase de Ataque

Fase de Coleta

Fase da Fraude

Fase Pós-ataque



A condução de um ataque tradicional

Fase de Planejamento:

- Definição do Alvo;
- Elaboração dos objetivos;
- Escolha da via a ser utilizada;
- Escolha dos métodos a utilizar;



A condução de um ataque tradicional



Fase de Preparação:

- Elaboração do material a ser utilizado;
- Obtenção de informações sobre o alvo.
- Preparação das máquinas e componentes eletrônicos a serem utilizados;
- Elevação do nível de ocultação;



A condução de um ataque tradicional



Fase de Ataque:

- Utilização da via escolhida na primeira fase.
- O ataque, propriamente dito.



A condução de um ataque tradicional

Fase de Coleta

Fase da Fraude:

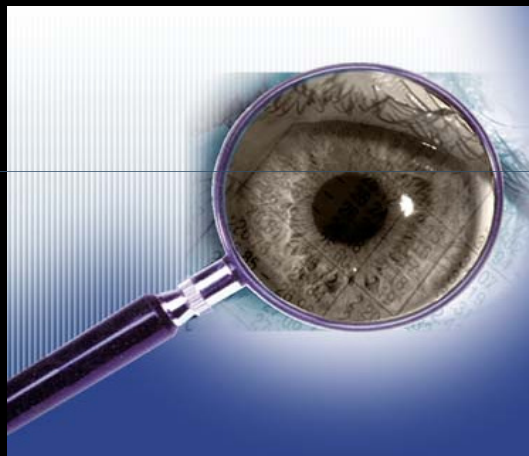
- Roubo de dinheiro, informações sensíveis, apropriação da identidade alheia (reutilizar ou vender).

Fase pós-ataque

- Destruição das evidências;
- Avaliação da efetividade;
- Possível lavagem de dinheiro;



Reconhecendo Phishing Scam



Um conhecimento fundamental.

Phishings, como qualquer outra cópia, sempre possuem falhas. Uns mais...





Departamento de Polícia Federal



Informativo

O departamento de polícia federal está fazendo enquetes contra hackers que invadem contas de bancos, os chamados "Crackers", ainda não existe uma lei fazendo se dirigindo totalmente á esses criminosos, esperamos por sua ajuda para votar e criar essa lei.

Baixe o programa para votação [aqui](#).

***Programa anti-hacker**

***Programa anti-spam**

***Programa anti-invasão**

A direção.

Obs: recomendamos o uso de nossos programas para poder prevenir os usuarios cada dia mais dos ataques hacker.



Ministério da Justiça



Reconhecendo Phishing Scam

Outros menos...



Assunto: Polícia Federal - Urgente

De: crimesdigitais@dpf.com.br

Data: 24-06-2006 04:13

Para: [REDACTED]



Departamento de Polícia Federal

Senhor/Senhora,

Você teve sua máquina logada em um site ilegal.

Precisamos que esclareça o fato o mais rápido possível, caso não seja esclarecido em 24 horas, um inquérito será aberto.

Para entrar em contato com o Departamento da Polícia Federal e esclarecer o acontecimento [clique aqui!](#)

Superintendente:

DPP Daniel Gomes Sampaio

Endereço:

SAIS Quadra 7 - Lote 23 - Setor Policial Sul Brasília-DF
CEP 70610-901

Fone:

(0xx-61) 33-45-9500



Reconhecendo Phishing Scam

Problemática: Como identificar?

1) Endereço do remetente:

Geralmente spoofados. Mas caso não correspondam ao original, é fator eliminatório.

2) Formatação e ortografia da mensagem:

Geralmente possuem falhas de formatação e ortografia, muitas vezes gritantes.



Reconhecendo Phishing Scam

3) Proposta ou requisição:

As propostas ou requisições são geralmente suspeitas:

- Solicitações repentinas com curto prazo;
- Solicitações ameaçadoras;
- Propostas de dinheiro fácil;
- Solicitações contraditórias;
- Dentre outras...

É um passo muito importante saber analisa-las.



Reconhecendo Phishing Scam

4) O endereço para o qual o link remete:

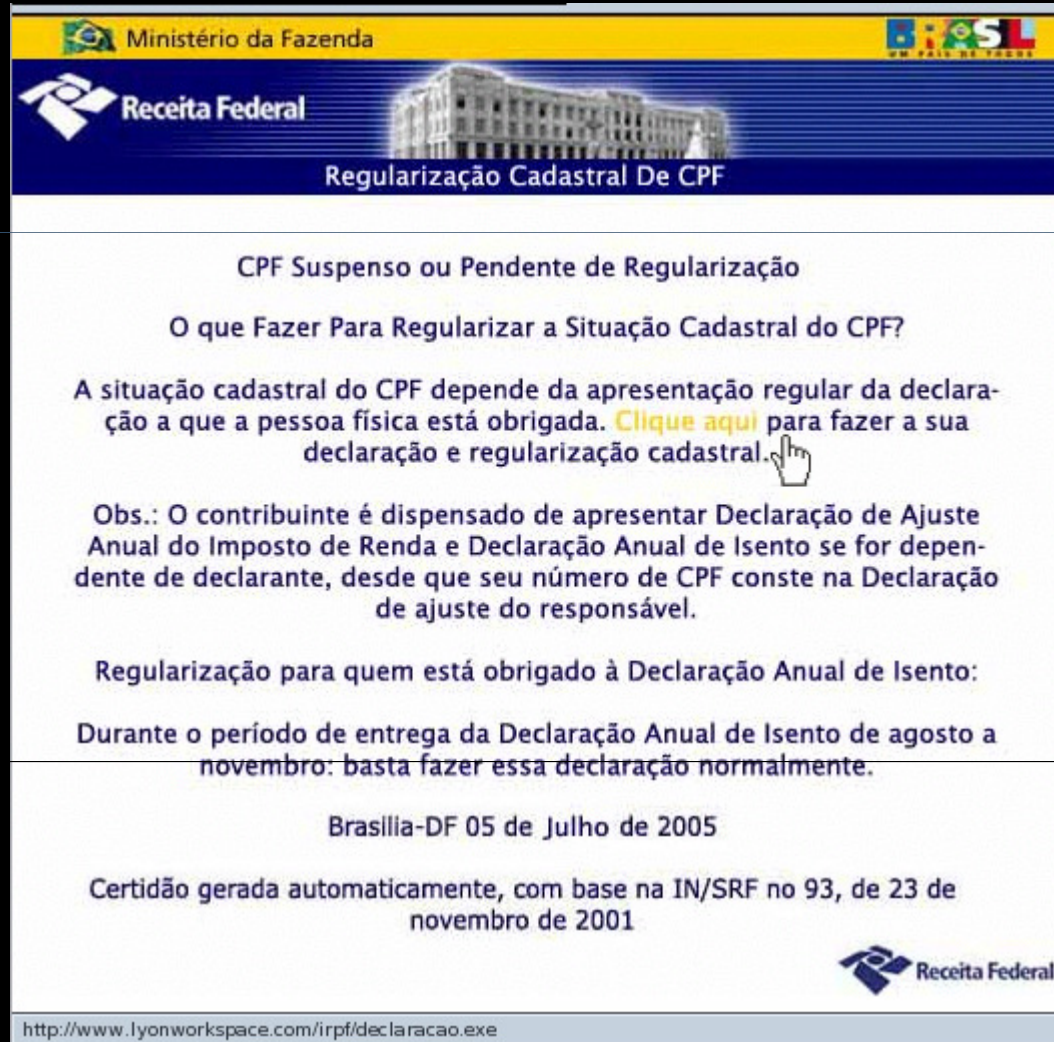
- Com frequência contêm downloads de arquivos de extensões suspeitas (.exe, .scr).
- Arquivos contraditórios.
- Pode ainda levar a páginas que sugiram ser autênticas, mas não o são.

Ex.: O texto exibido é www.gris.dcc.ufrj.br | Remete para www.grisdcc-ufrj.ru33.br.

- Verificação fundamental. Canto inferior esquerdo do navegador.
- *Atentar para URL's com hífen e/ou contendo IP's!!!*



Alguns casos de Phishing



Ministério da Fazenda

Receita Federal

Regularização Cadastral De CPF

CPF Suspenso ou Pendente de Regularização

O que Fazer Para Regularizar a Situação Cadastral do CPF?

A situação cadastral do CPF depende da apresentação regular da declaração a que a pessoa física está obrigada. [Clique aqui](#) para fazer a sua declaração e regularização cadastral.

Obs.: O contribuinte é dispensado de apresentar Declaração de Ajuste Anual do Imposto de Renda e Declaração Anual de Isento se for dependente de declarante, desde que seu número de CPF conste na Declaração de ajuste do responsável.

Regularização para quem está obrigado à Declaração Anual de Isento:

Durante o período de entrega da Declaração Anual de Isento de agosto a novembro: basta fazer essa declaração normalmente.

Brasília-DF 05 de Julho de 2005

Certidão gerada automaticamente, com base na IN/SRF no 93, de 23 de novembro de 2001

Receita Federal

<http://www.lyonworkspace.com/irpt/declaracao.exe>



VIRTUAL
CARDS
-COM-BROS CARTÕES MAIS
ANIMADOS DA WEB!

VIRTUALCARDS PARA Meu amor!!!

Tudo bem **Meu amor**?! Você acaba de receber um **VIRTUALCARDS**,
os cartões mais animados da Web, enviado por **Alguém que te ama**.
Para visualizá-lo, basta clicar no link abaixo e pronto!

[Clique aqui para visualizar o seu cartão](#)

Caso você não esteja conseguindo visualizar o cartão, por favor,
instale o plugin Macromedia Flash 5, clicando no botão abaixo.

VIRTUAL
CARDS
OS CARTÕES MAIS
ANIMADOS DA WEB!

Um grande abraço da Equipe VIRTUALCARDS.

Informações sobre este e-mail

Este e-mail foi gerado automaticamente. Não responda.

[| Termos do Serviço e Política de Privacidade |](#)

Copyright © 2001 - 2005 VITALEWEB - BRASIL
Todos os Direitos Reservados - All Rights Reserved



From: <net-informa5@uol.com.br>
Date: 2008/6/4
Subject: Veja a pessoa que voce ama e confia te traindo!!!
To: rio-pm-owner <rio-pm-owner@pm.org>

Ola como vai!

Oi, estou enviando esse e-mail, pois procurei outra forma de te avisar e não encontrei, nem queria ter que fazer isso. estou até meio sem jeito de não poder te falar pessoalmente, mais me sinto na obrigação de te avisar, não sei se você já ficou sabendo por alguém, mais saiba que a pessoa que você ama e confia esta lhe traindo...

É difícil de acreditar numa historia dessas mais como as imagens valem mais que as palavras, estou te enviando essas fotos q não sei porq mais chegaram ate mim, dai não tem como eu ficar de braços cruzados, então veja voce mesmo.

Clique no link abaixo para visualizar as fotos ou copie e cole o link no seu navegador.

<http://www.chinesefreewebs.com/fly1/?fotos.jpg>



Como proteger-se?

Software e Informação: O escudo e a muralha

- Phishing Scam utiliza-se de ataques a nível psicológico. Disto decorre a conclusão de que o uso de softwares, exclusivamente, não é o suficiente para proteger-se.
- Engenhosidade combate-se com engenhosidade.
- Se todos os softwares hoje fossem autosuficientes em resolver todos os problemas de segurança existentes no mundo digital, não haveria necessidade de tantos profissionais de SI, ou seja...



:x



Como proteger-se?

Software e Informação: O escudo e a muralha

- Escudo: Pode proteger de um, dois ou três adversários
 - Muralha: Pode proteger de um exército.
 - Aplicativos: 60 a 70% de eficácia
 - Indivíduo instruído: Pode chegar a 100%.
-
- Softwares anti-phishing trabalham sobre banco de dados. Decorrem 3 problemas:
 - Mensagens não reportadas – Não identificáveis.
 - A decisão final é sempre do usuário.
 - Anti-Phishings não cobrem todos os pontos suscetíveis. Ex: Vishing Scam.



Como proteger-se?

Software e Informação: O escudo e a muralha

- Embora os softwares não devam substituir a informação, é recomendável.
- Particularmente úteis em máquinas compartilhadas ou grandes grupos.
- Anti-phishings: Geralmente integrados a outros aplicativos. Ex: Browsers – Firefox



Scam Baiting: Divertindo-se com o inimigo

“O maior prazer de um Homem inteligente é fazer-se de idiota frente a um idiota que se faz de inteligente.”

Phishers são indivíduos maliciosos, que jogam com suas vítimas.
Mas o que acontece quando a vítima também sabe jogar?



Scam Baiting: Divertindo-se com o inimigo

- Não possui tradução exata. Corresponde a “apresentar uma isca ao atacante”.
- Particularmente utilizado no caso de fraudes 419 (Longo jogo de e-mails).
- O objetivo do atacante: Fraudar.
- Seu objetivo: Se divertir! Induzir o phisher a gastar recursos e expor-se ao ridículo.
- Desvia a atenção do phisher, que poderia estar voltada a um usuário inocente.
- Regra básica: **JAMAIS** exponha quaisquer dados pessoais reais, ou permita-se um encontro ao vivo.
- Outras regras, dicas e informações: 419 eater (www.419eater.com)



Scam Baiting: Divertindo-se com o inimigo

Vê como pode ser divertido?



Recomendações Diversas



1) Suspeite!

2) Em caso de dúvida, confirme!

3) Use o Google!

4) Verifique atentamente a extensão do arquivo!

5) Se possui conhecimentos, pratique Scam Baiting



Recomendações Diversas



- 6) Treine seu grupo
- 7) Utilize filtros anti-phishing
- 8) Utilize anti-virus, firewall e anti-spyware
- 9) Leve a informação adiante!
- 10) Reporte!



Reportando



- Importante para a comunidade de S.I., importante para você.
- Reportar: APWG (Anti-Phishing Working Group) em reportphishing@antiphishing.org.
- No caso de uma empresa, reportar ao CSIRT (caso exista).



Quando já é tarde

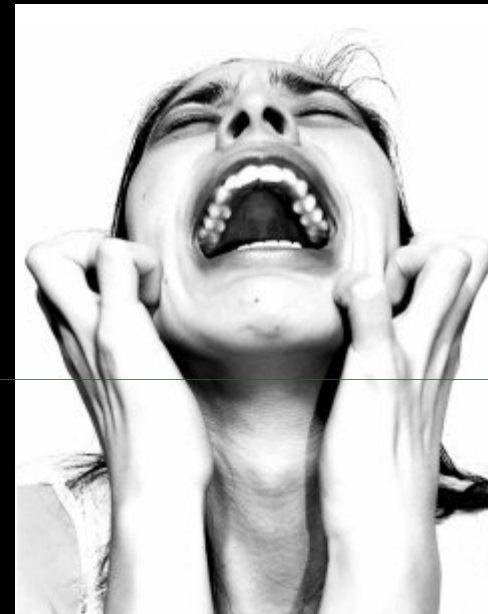
Mordi a isca, e agora?!

Ficar estático e lamentar não é a postura correta a se assumir.

Primeiramente, reportar o incidente:

- À sua companhia de cartões de crédito;
- À companhia que você julga ter sido forjada;
- Opcionalmente, porém recomendável, reportar ao APWG em: http://www.antiphishing.org/report_phishing.html.

- Alterar todas as senhas, começando por aquelas que têm relação com instituições financeiras. Opte por utilizar senhas fortes.



Quando já é tarde

Mantenha as próximas faturas de seus cartões de crédito e o extrato de sua conta sob observação, de modo a perceber alterações ou transações que você não realizou.

E, por fim, proteja-se:

Informe-se e mantenha-se atento, alertando e instruindo ainda ao máximo de indivíduos possível.



Fim

Dúvidas???



diego@gris.dcc.ufrj.br
<https://www.gris.dcc.ufrj.br>

