
Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

**CLEBER GUEDES PEREIRA**

# *PHISHING*: CONCEITOS E AÇÕES PREVENTIVAS APLICADAS À EMPRESA.

**Brasília**

**2012**

**CLEBER GUEDES PEREIRA**

# *PHISHING*: CONCEITOS E AÇÕES PREVENTIVAS APLICADAS À EMPRESA.

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. Msc. Marco Antonio Araújo

**Brasília**

**2012**

**CLEBER GUEDES PEREIRA**

# *PHISHING*: CONCEITOS E AÇÕES PREVENTIVAS APLICADAS À EMPRESA.

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Redes de Computadores com Ênfase em Segurança.

Orientador: Msc. Marco Antonio Araújo

Brasília, 31 de Outubro de 2012.

**Banca Examinadora**

_____

Prof. Msc. Marco Antonio Araújo

_____

Prof.ª Dra. Tânia Cruz

_____

Prof. Dr. José Eduardo M. S. Brandão

## AGRADECIMENTO

Agradeço primeiramente a Deus, pela força, paciência e perseverança que consegui ao longo desse trabalho. Aos meus pais, Bartolomeu e Cleta, que com muito carinho sempre incentivaram e acreditaram no meu potencial.

À minha irmã Kelvia, minha esposa Vilmara, minha filha Ludmila, que com muita compreensão me apoiaram e não mediram esforços para que eu chegasse até esta etapa de minha vida.

Agradeço a instituição EMBRAPA – Empresa Brasileira de Pesquisa Agropecuária e a unidade descentralizada CNPH - Centro Nacional de Pesquisa de Hortaliças, que através do programa de pós-graduação Lato Sensu, me conferiram a oportunidade de cursar essa especialização.

Aos colegas de trabalho, Roberto Cesar, Cleone Silvestre e Haldane Capanema pelo incentivo, cumplicidade e amizade.

Ao professor Marco Antonio pela orientação desse trabalho, e ao coordenador professor Francisco Javier por todo apoio prestado.

A todos que de alguma forma contribuíram para o desenvolvimento desse trabalho.

## RESUMO

Paralelamente ao crescimento da tecnologia da informação tem ocorrido também o aumento no número e modalidades de ataques cibernéticos, que ameaçam a segurança das informações tanto no ambiente domiciliar quanto no corporativo. Dentre essas ameaças destaca-se o phishing, termo originado da palavra em inglês fishing que significa pescar. É uma forma de fraude eletrônica cujo objetivo é obter informações pessoais dos usuários como cartões de crédito e senha e utilizá-las com outros fins. Como o termo sugere, phishing é uma tentativa de o fraudador "pescar" as informações dos usuários inexperientes. Desta forma é primordial e urgente que a empresa disponha de sistemas protegidos e de usuários conscientes e treinados acerca do tema em questão. Com base nisso é objetivo desse trabalho demonstrar o funcionamento da fraude online phishing e propor a redução da incidência desse tipo de ameaça de forma a não impactar na continuidade dos negócios da empresa. Vamos elencar os tipos de fraudes envolvendo phishing e propor através do uso das melhores práticas de segurança da informação, apoiados na norma NBR ISO/IEC 17799/2005 uma proposta para treinamento e conscientização do usuário de TI de uma empresa, frente às ameaças de phishing.



**Palavras Chave**: Segurança da Informação, Phishing, Empresa, Ações Preventivas.

**ABSTRACT**

In parallel with the growth of information technology has also occurred the increase in the number and types of cyber-attacks, which threaten the security of information both in the home environment as in corporate. Among these threats stands out phishing, term originated the word in english fishing which means fish. It is a form of electronic fraud whose goal is to obtain personal information of users such as credit card and password and use them for other purposes. As the term suggests, phishing is an attempt of the swindled "fish" the information on users inexperienced. In this way is vital and urgent that the company has protected systems and users aware and trained about the topic in question. On the basis and purpose of this study demonstrate the operation of online fraud and phishing propose to reduce the incidence of this type of threat in such a way as to not impact on continuity of the company's business. Let's list the types of fraudulent phishing and propose through the use of best practices in information security, supported by the NBR ISO / IEC 17799/2005 a proposal for training and user awareness of an IT company, in the face of threats of phishing.

**Keywords**: Information Security, Phishing, Business, Preventive Actions.

**LISTA DE FIGURAS**

Figura 1 - Funcionamento do Sender ID..... 31

Figura 2 - Processo de Autenticação de Mensagem do DMARC..... 36

**LISTA DE TABELAS**

Tabela 1 - Tendências geográficas..... 13

Tabela 2 - Tendências de mercado..... 13

Tabela 3 - Tendência vertical.....14

Tabela 4 - Comparativo entre as técnicas.....37

**SUMÁRIO**

INTRODUÇÃO ..... 10
Cenário Atual ..... 12
Estrutura do Trabalho ..... 14
CAPÍTULO 1 – CONCEITOS DE PHISHING ..... 16
1.1 Características do *Phishing* ..... 16
1.2 Métodos mais usados de phishing ..... 17
1.2.1 Pharming ..... 17
1.2.2 Spear Phishing ..... 18
1.2.3 iPhishing ..... 19
1.2.4 Vishing Scam ..... 20
1.2.5 Mensageiro Instantâneo ..... 21
1.2.6 Sites de Relacionamento ..... 22
1.3 As Fases de um Ataque ..... 23
1.4 Prejuízos com o Phishing ..... 25
CAPÍTULO 2 - TÉCNICAS DE DEFESAS PARA O PHISHING ..... 28
2.1 Ferramentas nas Empresas ..... 28
2.1.1 SPF ..... 28
2.1.2 Sender ID ..... 30
2.1.3 DomainKeys ..... 32
2.1.4 DKIM ..... 33
2.1.5 DMARC ..... 35
2.1.6 Comparativo entre as Técnicas ..... 37
2.2 Como Identificar a Fraude de Phishing ..... 38
2.3 O que Fazer Com um Caso de Phishing ..... 39
2.4 Recomendações de Segurança ..... 40
CAPÍTULO 3 - CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE A SEGURANÇA NA EMPRESA - UMA PROPOSTA ..... 42
3.1 Cultura de Segurança ..... 42
3.2 Adoção de Boas Práticas de Segurança ..... 43
3.3 Proposta do Programa de Conscientização ..... 45
3.3.1 Metodologia de Implantação ..... 46
3.3.2 Programa de Conscientização ..... 47

CONSIDERAÇÕES FINAIS ..... 52
REFERÊNCIAS ..... 53

## INTRODUÇÃO

Quando falamos em tecnologia da informação (TI) é fundamental nos remetermos também à questão da segurança dos dados. A expansão tecnológica proporcionou uma "popularização" da informática e consequentemente uma maior exposição a ataques cibernéticos, principalmente às empresas, sejam de pequeno, médio ou grande porte.

Nos primeiros anos em que ocorreu a informatização das empresas, onde os recursos materiais eram demasiadamente "caros" e os recursos humanos especializados ainda escassos, as informações eram concentradas em uma espécie de "central", na qual eram armazenados todos os dados de maior importância e de sigilo e de acesso restrito a um indivíduo ou a um numero pequeno de pessoas. O avanço dos recursos tecnológicos e da acessibilidade contribuiu para a modernização das empresas possibilitando a ampliação e descentralização dos dados. No entanto, grande parte dos usuários continua despreparada frente ao manejo seguro das informações (OLIVEIRA; VIEIRA, 2011).

Grande parte das empresas que tem sido alvejadas armazenam em seus arquivos eletrônicos um grande número de dados, muitas vezes desprovidos de sistemas de segurança confiáveis, haja vista o número de ataques registrados nos órgãos competentes como o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil ( CERT.br ) (CERT.br, 2012), os quais serão também demonstrados em seção distinta deste trabalho.

Os "hackers" se aproveitam de "falhas" nos diversos setores desde o despreparo do usuário/cliente, fatores físicos como a radiação ou mesmo falhas nos softwares, os quais permitem o acesso do agente criminoso aos dados da empresa. Desta forma, é fundamental que a segurança no ambiente de TI seja garantida por que fortaleçam e protejam contra esses acessos indevidos, alterações de dados e outros danos aos sistemas de informação. Baseado nessa visão, cada vez mais as empresas tem investido na modernização dos sistemas, lançando

mão de políticas, técnicas e procedimentos específicos no que diz respeito à manipulação dos dados (LAUDON; LAUDON, 2007).

A vulnerabilidade na segurança pode ter sua origem em de fatores técnicos, organizacionais e ambientais, agravados por decisões administrativas erradas. Os usuários/clientes podem contribuir com as falhas e danos ao introduzir erros ou ao acessar sistemas sem autorização. Aproveitam-se ainda de interrupções na rede originárias da radiação para instalar softwares intrusos, destruindo ou alterando dados corporativos e causando erros no sistema como um todo. Há ainda as causas de falha em softwares, geralmente erros de programação e instalação ou alterações não autorizadas. Também não se deve esquecer que os diversos fenômenos naturais podem afetar os sistemas de computador (UNIESP, 2011).

O acesso irrestrito à rede mundial de computadores – Internet – também representa fator de risco para as informações, pois como é uma rede pública e, portanto acesso livre de qualquer usuário, aumentando a vulnerabilidade a abusos diversos de consequências por vezes desastrosas. Além disso, os computadores, uma vez ligados à internet por endereço fixo, podem ser facilmente rastreados e identificados, tornando-se alvos para infratores.

No encalço do avanço tecnológico e das políticas de segurança os criminosos também têm buscado cada vez mais novas técnicas para invadir os computadores e acessar os dados sigilosos tanto do usuário domestico como das empresas. Uma das técnicas mais utilizadas atualmente é o *phishing,* onde o fraudador cria uma página falsa baseada em páginas oficiais de instituições bancárias renomadas. Estas páginas são enviadas via email e contém mensagens nas quais os usuários são induzidos a fornecer informações pessoais e confidenciais principalmente senhas bancárias e números de cartões de crédito bem outras informações, que posteriormente são utilizadas pelo criminoso (JUNIOR; LIMA, 2010).

Considerando-se este cenário são objetivos deste trabalho:

- Demonstrar o funcionamento da fraude online *phishing* e propor a redução da incidência desse tipo de ameaça de forma a não impactar na continuidade dos negócios da empresa.
- Elencar os tipos de fraudes envolvendo *phishing*;
- Propor uso das melhores práticas de segurança da informação, a fim de evitar o uso abusivo e fraudulento dos recursos de Tecnologia da Informação (TI) nas empresas.
- Apresentar uma proposta para treinamento e conscientização do usuário de TI de uma empresa, frente às ameaças de *phishing*.

**Cenário Atual**

O crescimento dos ataques de *phishing* é um fator de grande preocupação no universo da segurança de dados. Os relatórios de órgãos como o *Anti-Phishing Working Group* **(**APWG, 2012), CERT.br (CERT.br, 2012) e *Symantec* (SYMANTEC, 2012) tem demonstrado que esses ataques tem obtido êxito acima do esperado, representando um desafio para os técnicos em TI.

O APWG é um consórcio sem fins lucrativos compostos por bancos, fornecedores de segurança e outras empresas do ramo e aponta que o índice de sucesso dessa técnica ultrapassa os 5%.

Dados recentes do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), apontam que os incidentes de fraudes no segundo trimestre de 2012, aumentaram significativamente. Os números de tentativas de phishing foram maiores em relação ao primeiro trimestre. Houve um aumento de 89% no número de notificações de paginas falsas de instituições financeiras e sites de comercio eletrônico. Em comparação com

mesmo período de 2011, o crescimento foi de 184%. Foi identificado também um aumento de 4% no número de notificações de páginas falsas não relacionadas a serviços financeiros ou comércio eletrônico, em comparação com o mesmo período de 2011.

O relatório de Junho/2012, da SYMANTEC (2012), empresa de segurança da informação, apresenta um crescimento de 0,04 % no registro do *phishing*. Os e-mails contendo alguma espécie de ameaça foi para um a cada 467,6 e-mails demonstrando aumento em relação ao mês de Maio do corrente ano quando a proporção registrada foi de um a cada 568 emails. Tomando-se uma tendência geográfica temos o seguinte cenário:

**Tabela 1: Tendências Geográficas**

| **País** | **Proporção de Phishing** |
|---|---|
| Holanda | 1:54,4 |
| Canadá | 1:332 |
| Brasil | 1:713 |
| Alemanha | 1:1.043,7 |
| Estados Unidos | 1:1.261,5 |

**Fonte: SYMANTEC(2012)**

Ainda segundo o mesmo relatório pequenas empresas são alvo de quase um terço dos ataques direcionados, isso significa que os criminosos estão mudando de atitude e transferindo seus ataques para empresas de pequeno porte. Porém isso não significa que empresas maiores estão fora de sofrer ataques, pois elas podem esta sendo usada como degrau para atacar empresas menores.

**Tabela 2: Tendências de Mercado**

| **Proporção de E-mails Bloqueados como Phishing** | |
|---|---|
| **Tipos de Empresa** | Maio/2012 |
| Pequenas/Medias | 1:450,6 |
| Grandes | 1:540,6 |

**Fonte: SYMANTEC(2012)**

Analisando os dados considerando a natureza de operações podemos agrupar os dados na seguinte tabela:

**Tabela 3: Tendência Vertical**

| Setor | Proporção de Phishing |
|---|---|
| Finanças | 1:247,5 |
| Educação | 1:330,6 |
| Varejo | 1:835,3 |
| Serviços de TI | 1:986,8 |
| Indústria Química e Farmacêutica | 1:1.201,2 |
| Setor Automotivo | 1:2.114.3 |

**Fonte: SYMANTEC(2012)**

## Estrutura do Trabalho

No primeiro capítulo apresentamos a teoria acerca do *phishing*, técnicas de engenharia social e os conceitos básicos sobre o assunto. Em seguida são mostrados os métodos de phishing mais usados pelo cibercriminosos e como eles agem detalhando todas as suas fases, finalizando com os prejuízos causados pelos ataques no Brasil e no mundo e quais as categorias da economia são mais afetadas.

O segundo capítulo explana sobre as opções de técnicas de defesa contra o *phishing* apresentando as ferramentas disponíveis e mais utilizadas pelas empresas e como elas funcionam. A seguir é demonstrada como pode ser feito um trabalho de conscientização sobre cultura de segurança na empresa com uso das boas práticas de segurança conforme a norma NBR ISO/IEC 17799/2005 (ABNT, 2005) principalmente em relação aos controles com relação a treinamento de pessoas e serviços de email.

No terceiro capitulo é apresentada então, uma proposta de treinamento para usuário de empresas, com base nas recomendações da NBR ISO/IEC 17799/2005 com foco na conscientização da segurança da informação e ameaças oriundas de e-mails. No detalhamento deste capitulo é demonstrado as fases do programa de conscientização e como

será feito a aplicação dessa proposta. Nas considerações finais são apontadas as principais vantagens de se fazer o programa de conscientização aos funcionários e como isso contribuirá para uma maior segurança das informações nas empresas.

# CAPÍTULO 1 – CONCEITOS DE PHISHING

## 1.1 Características do *Phishing*

Com a dependência cada vez maior dos sistemas informatizados, e o surgimento de novas tecnologias, aumentaram os problemas de segurança devido ao crescimento do número de vulnerabilidades. (OLIVEIRA; VIEIRA, 2011).

Atualmente, existem técnicas de roubos de informações, em que o foco está em enganar o usuário e explorar vulnerabilidade nos sistemas de informação. Essa técnica é chamada de Engenharia Social (BRAGA, 2010).

"Engenharia Social é a 'arte' de utilizar o comportamento humano para quebrar a segurança sem que a vítima sequer perceba que foi manipulada". Ou seja, os indivíduos, fornecem informações importantes facilmente por confiarem nas outras pessoas. Indivíduos mal intencionados utilizam-se da Engenharia Social para conseguir informações sobre o usuário e então preparar e efetivar seus ataques (OLIVEIRA; VIEIRA, 2011).

De acordo com Laudon e Laudon (2007), as técnicas mais usadas pelos hackers são os sites falsos e os emails contendo phishing. Essas mensagens servem para capturar as informações e dados pessoais, como CPF, nome, senha e depois são utilizadas de forma fraudulentas.

Segundo Olivo (2010), *phishing* é a técnica que se utiliza da engenharia social para fazer suas vítimas, persuadindo-os com objetivos de capturar as informações pessoais e depois usa-las de forma a causar-lhes prejuízos. O mecanismo básico encontra-se descrito da seguinte forma:

> Na internet, o phishing pode chegar ao usuário (vítima) de várias maneiras, através de uma janela pop-up no navegador (browser), de mensagens instantâneas ou de

> emails. Geralmente, a vítima é convencida a executar um clique de mouse, que descarregará e instalará algum malware (código malicioso) ou acessará um site fraudulento.

Para Olivo (2010), o *e-mail* é o serviço de Internet mais utilizado atualmente, e suas características por si só já permitem as ações criminosas por esse motivo é largamente utilizado para veicular o *phishing*.

A maioria dos clientes de email suporta HTML, o que possibilita que todos os recursos disponíveis na linguagem HTML feitos para páginas na WEB fiquem disponíveis para emails. Com isso um *hyperlink* ( link usado em hipertexto, para ligar um texto visível a um endereço "invisível"), ambos se tornaram uma poderosa ferramenta para os *phishers*.

Segundo Beal (2008) apud Silva (2008), a tecnologia da informação traz para as empresas como grande benefício, uma maior qualidade e disponibilidade de informações e conhecimentos essenciais para a organização.

## 1.2 Métodos mais usados de phishing

Um *Phishing* pode ser realizado de diversas maneiras. As mais comuns são:

### 1.2.1 Pharming

Essa técnica explora uma vulnerabilidade do sistema DNS ( Servidor de Nomes de Domínios ) conhecida também como DNS *cache poisoning*. O servidor DNS é o responsável em traduzir uma URL (Localizador Padrão de Recursos) em endereço de

máquina, ou IP( *Internet Protocol* ), por exemplo, ao digitar www.google.com.br o sistema DNS é responsável por traduzir e direcionar para o IP 74.125.234.

Caso o servidor DNS esteja vulnerável, o endereço digitado poderá ser direcionado para uma página falsa hospedada em outro servidor com outro endereço IP. Essa ação é feita de forma automática, sem interação ou que usuário tome conhecimento que foi redirecionado para site não legitimo. É uma técnica muito difícil de ser detectada pelo usuário (PAIVA, 2007).

### 1.2.2 Spear Phishing

Para a COMPUTERWORLD (2012), estudo da empresa fabricante de soluções de segurança TrendMicro, aponta que:

> Do ponto de vista empresarial, as novas tendências no cenário de spams e fraudes vão além da inundação usual de e-mails em massa e incluem agora o "spear-phishing", utilizado por cibercriminosos que desejam obter acesso a alvos específicos da organização.

*Spear Phishing* é um ataque de *phishing* altamente focalizado, com foco em grandes organizações e exige um estudo detalhado por parte dos atacantes. Fazendo uma correlação entre "*phishing*", sua denominação pode ser entendida como "a pesca de arpão" (MARTINS, 2008).

Inicialmente é estabelecido o alvo, que geralmente pode ser um departamento, ou ainda instituições governamentais ou bancárias. Logo depois se faz um levantamento sobre as informações de cada funcionário em diferentes setores.

Nesse tipo de ataque, explora-se o fator falha humana, principalmente a dificuldade de avaliar corretamente a veracidade de uma informação. Uma única informação, pode não ter muito significado, mas uma vez de posse de indivíduos mal intencionados, pode ocasionar inúmeros prejuízos como, por exemplo, até mesmo possibilitar que o criminoso se passe por um funcionário da alta diretoria.

Nesta fase o *phisher* se molda de acordo com o dia a dia da empresa, absorvendo os jargões e assimilando os processos e procedimento internos. Isso pode demorar vários dias, e até lá o *phisher* pode ser passar por várias pessoas da empresa, até que encontre a informação que deseja ou a pessoa certa para concluir seu ataque.

Atingido o seu objetivo, o atacante passa a ter acesso a toda rede da empresa, com acesso a informações sigilosas e poder de realizar transferências ou pagamento por exemplo.

### 1.2.3 iPhishing

A popularização do acesso a internet e a chegada de diversos dispositivos como *tablets*, *smartphones* e televisores interativos que acessam a internet, fez com que a atenção ficasse voltada ao designer e tecnologias desses aparelhos, todavia os aspectos como a segurança das informações foi deixada para segundo plano (NIU, 2008).

Alguns aspectos físicos como tamanho da tela, dificultam a visualização de urls, além de possibilitar maior facilidade para navegação por link, que deixam o usuário mais propenso a cair em um golpe de *phishing*. Além disso, a atualização de segurança, item de muita importância para bom funcionamento do sistema, se torna tarefa árdua, já que esse processo não é tão fácil de realizar comparados com um desktop.

Para Martins (2008*)* a definição de *iPhishing* é dita da seguinte forma;

> É a vertente que visa explorar vulnerabilidades conseqüentes do avanço excessivamente rápido da tecnologia, que acaba por deixar aspectos de segurança em segundo plano, dando lugar à funcionalidade e ao design.

Uma forma de ataque comum nesses dispositivos é o uso do método do Javascript, chamado scrollto(). Nesse método, no momento que a página se carrega, ela pula para outra área de mesma tela, impossibilitando assim que se a URL possa ser visualizada. A cada vez que se tenta ver o topo da página, o usuário é lançado para outro ponto da página.

Dessa forma, essa técnica ainda será bastante explorada por criminosos, tendo em vista que o lançamento de novas tecnologias ou produtos, sempre virá acompanhado de grandes vulnerabilidades.

### 1.2.4 Vishing Scam

A chegada de novas tecnologias normalmente vem acompanhada das possibilidades de serem exploradas e utilizada de forma errada. Segundo Martins (2008), a tecnologia VOIP ( *voice over* IP), que permite comunicação utilizando rede internet baseando-se no IP ( protocolo Internet) e possibilita que se façam ligações com baixo custo mascarando o telefone de origem. No entanto, o *hacker* enxerga no VOIP uma ferramenta para implementação de novas ações baseados no *phishing* tradicional (MARTINS,2008).

Na execução desse ataque, o atacante começa com o envio diversas mensagens de texto (SMS), email ou até mensagens de voz para o celular da vitima. Então utilizando da técnica de engenharia social, ele convence a usuário a ligar para um número, oferecendo para

isso várias vantagens e prêmios, e também o amedrontando, com garantia de que sua conta esta suspensa e para reativa-la é preciso de confirmação de alguns dados.

Uma vez convencido, e a ligação efetuada, a vitima é atendida por uma central telefônica, chamadas de ura, que pedem para digitar seus dados pessoais, como conta bancária e senha de acesso. Confirmada a inserção dos dados, o ataque de *Vishing Scam* está completo. Com base nestas informações, o hacker então poderá clonar cartões de crédito ou efetuar transações financeiras.

Existem formas agressivas de ataques de *Vishing Scam*. Utilizando-se de scripts, os atacantes iniciam chamadas VoIP para vários telefones de uma mesma faixa de números. Pode-se mascarar o numero de origem da ligação e parecer ser de uma instituição genuína. Caso a ligação do atacante seja direcionada a uma caixa de mensagens, uma mensagem é gravada solicitando que ligue para determinado numero para que se possam digitar os dados. Atualmente as mensagens de voz distribuídas de forma massiva denomina-se SPIT ( *Spam over Internet Telephony* ).

Ainda segundo o mesmo autor, os ataques de *Vishing Scam* crescem tanto em quantidade e sofisticação. No Brasil, esse tipo de ataque não é muito utilizado, tendo em vista que a tecnologia VOIP ainda não é muito popular, mas com certeza nos atingira em um futuro breve.

### 1.2.5 Mensageiro Instantâneo

Os emails e serviços de mensagens instantâneas representam uma das principais ferramentas de comunicação na vida moderna e consequentemente um dos meios mais utilizados pelos *phishers* para atingir os usuários. Pode-se afirmar que os usos indiscriminados desses recursos estão relacionados diretamente à disseminação do *phishing*,

pois a estas mensagens podem ser anexados arquivos e links não confiáveis e danosos, conforme nos relata Martins (2008).

Os criminosos utilizam-se da informalidade desse tipo de comunicação para simularem um falso vínculo com o usuário que acaba sendo ludibriado e abrindo os anexos corrompidos, imaginando terem sido enviados por amigo ou familiar. A simultaneidade que este tipo de mensagem oferece para enviar URL's suspeitas que uma vez abertas acaba por "infectar" o usuário distraído.

No entanto um dos fatores que mais tem contribuído para o sucesso do phishing seja a inexperiência do usuário. A realidade é que o maior percentual dos clientes dos softwares instantâneos sejam crianças, adolescentes e leigos, com imaturidade no discernimento de links duvidosos e inadvertidamente infectam suas máquinas.

### 1.2.6 Sites de Relacionamento

A vulnerabilidade nesse tipo de site é semelhante ao item anteriormente abordado, com o adicional de que permite acesso público e a possibilidade do *phishing* atingir muitos outros indivíduos. Os criminosos exploram essa fragilidade e a curiosidade das pessoas. Por exemplo, podem ser enviadas mensagens de que existe foto, vídeo ou notícias difamadoras a respeito do usuário, instigando-o a clicar no link (MARTINS, 2008). Ao clicar é então imediatamente redirecionado para um site fraudulento muito semelhante ao original, onde é impelido a digitar senhas ou instalar outros softwares que tem a real intenção de roubar informações acerca desse usuário.

## 1.3 As Fases de um Ataque

Os *phishers* utilizam inúmeras formas para realizar seus ataques, seja enviando mensagens do tipo Spam ou focalizando os mesmos, neste caso, conhecidos como *Spear Phishing.* Porém, independente da sua natureza esses ataques geralmente possuem sempre alto nível de sucesso, ultrapassando os 5%, de acordo com o *Anti-Phishing Working Group* ( MARTINS, 2008).

### 1.3.1 Fase de Planejamento

Fase onde o atacante planeja como será toda a sua ação. É nessa fase, que é decidido qual o alvo e é elaborado o objetivo do ataque, de que artimanhas vai se valer e o qual método irá utilizar.

### 1.3.2 Fase de Preparação

Fase onde é confeccionado todo material que será utilizado no ataque, como coleta de emails, criação de sites falsos, etc. Levantam-se informações a respeito do alvo, monta toda parte eletrônica como equipamentos, criação de rede e servidores. Fase muito importante para que o ataque seja bem sucedido.

### 1.3.3 Fase de Ataque

Nessa fase onde ocorre o ataque propriamente dito, onde é utilizada toda estrutura previamente preparada na fase. O ataque pode ocorrer por email, através de um site, por mensageiros instantâneos, via VOIP e com distribuição de *malwares*.

### 1.3.4 Fase de Coleta

Fase que ocorre a coleta das informações obtidas com o ataque. São recuperados os dados inseridos nas páginas adulteradas, em resposta às mensagens disparadas por email ou capturadas por *malwares*.

### 1.3.5 Fase da Fraude

Nessa fase onde ocorre a fraude. Nela acontece o roubo de informações sensíveis, roubo de dinheiro e de identidade, vendas das informações a quem interessar ou usar esses dados em outros ataques.

### 1.3.6 Fase Pós-ataque

Ocorre perda de provas do ataque e da fraude. Nesta fase as máquinas são desligadas e qualquer rastro é eliminado. Existem também avaliação e balanço da ação, além de lavagem dinheiro, caso o ataque tenha ocorrido para esse fim.

## 1.4 Prejuízos com o Phishing

É inegável a magnitude dos prejuízos ocasionados pelas ações phishing. Segundo a fabricante de soluções de segurança TrendMicro, os recebimentos de mensagens com algum teor malicioso custaram US$ 2,8 bilhões em perda de produtividade as empresa européias e US$ 20 bilhões às norte-americanas. Já no Brasil, se prevê que as fraudes bancárias através da Internet causem prejuízo anual de aproximadamente R$ 1 bilhão, segundo a ONG de segurança da informação *Safernet*. Enquanto que, segundo levantamento divulgado pelo jornal O Globo, o setor bancário é um dos que mais recebe reclamações. Todas essas fraudes ocorrem por meio do ataque de *phishing* (COMPUTERWORLD, 2012).

Estima-se ainda que mais de 50% do trafego mundial de correio eletrônico é considerado spam. Mais alarmante é a sua taxa de crescimento: em 2001, esse tipo de fraude representava “apenas” 7% de todo o trafego mundial de correio eletrônico (CCE, 2004 apud ZUCCO,2005). Segundo NIC.BR (2012), assim como o *spam* o *phishing* também pode causar alguns problemas para os usuários da internet. Os prejuízos podem ser:

- Não recebimento de e-mails. Grande parte dos provedores limita o tamanho da caixa postal do usuário no servidor. Caso o recebimento de spam ou phishing seja grande, deixando as caixas postais ficarem cheias, e o servidor pode não permitir mais o envio nem recebimento de emails a partir de então;
- Desperdício de tempo. Tempo gasto pelo usuário para receber email, ler, analisar, identificar e mover para o lixo aquela mensagem que trata de *spam/phishing*.
- Gastos desnecessários. Seja qual for a forma de acesso do usuário a seu email, de certa forma ele está pagando a conta para ler aquele *spam/phishing*. Imagine um

usuário com internet discada, e gastando alguns minutos a mais para ler aquela mensagem indesejada.

- Perda de produtividade. Quem trabalha diariamente com email, como ferramenta de trabalho, o recebimento de mensagens indesejadas aumenta seu tempo gasto com leitura de emails, além de ter a possibilidade de que ele se engane e não leia mensagens importante ou atrase a resposta de um email legitimo;

- Perda de confiança. A um nível mais abrangente, o recebimento de spam/phishing diminui a confiança dos usuários, a qual se estabelece como um requisito para o sucesso das negociações no comercio e dos serviços eletrônicos.

E também segundo NIC (2004 apud ZUCCO,2005) para os provedores de acesso, backbones e empresas, o *spam/phishing* pode causar:

- Impacto na banda. O *spam/phishing* gerado aumenta o trafego de informações e obriga os provedores e empresas a aumentarem a capacidade de seus links com a internet. Isso reflete diretamente no bolso do usuário, tendo em vista que o custo desses links são muito alto e os provedores são obrigados a diminuir seus lucros, aumentando o custo para o usuário;

- Ma utilização dos servidores. Além do espaço gerado nos servidores oriundos de mensagens indesejadas como o *spam e phishing*, eles dedicam boa parte do tempo de processamento para tratar das mensagens não solicitadas;

- Perda de clientes. Os clientes se sentem afetados pela grande quantidade de spam que recebem ou tem seus envios de emails bloqueados em virtude de outros usuários que abusam daquele servidor de email. Dessa forma, muitas vezes o provedor perde seus clientes de maneira abrupta;

- Investimento em pessoal e equipamentos. Para melhor tratamento dos casos de *spam* e *phishing*, as empresas e provedores precisam contrata técnicos ou empresas especializadas para acrescentar mais ferramentas e sistemas de filtram, o que normalmente envolve compra de novos sistemas, treinamento e equipamento.

# CAPÍTULO 2 - TÉCNICAS DE DEFESAS PARA O PHISHING

## 2.1 Ferramentas nas Empresas

Os e-mails indesejados (Spam), e os ataques de phishing, atingem tanto os internautas domiciliares quanto os serviços de correio eletrônico das empresas. Existem vários métodos anti-spam e anti-phishing que uma vez bem implantados melhoram bastante os índices de sucesso dos ataques cibernéticos. O simples bloqueio da origem da mensagem não é recomendado porque é muito fácil falsificá-la. Existem métodos mais eficazes e inteligentes de obter sucesso, tais como o uso de SPF (*Sender Policy Framework*) (WONG, 2006), Sender ID (LYON, 2006), DKIM (*Domainkeys Identified Mail*)(CROCKER, 2011) e o um novo padrão que esta sendo adotado por grandes corporações como o Google, Microsoft, Yahoo, facebook e é chamado DMARC ( *Domain-based Message Authentication, Reporting & Conformance*)(KUCHERAWY, 2012). Segundo a APWG (2012) estima-se que a adoção de um ou dois desses padrões de autenticação de e-mail, poderiam bloquear em até 85% os ataques de *phishing* na sua forma básica.

### 2.1.1 SPF

O SPF - *Sender Policy Framework* – foi iniciado com o propósito de ser um padrão da IETF para habilitar validação de fontes do e-mail. O SPF tem como grande objetivo o combate a falsificação de endereços de retornos de e-mail. É uma técnica que permite definir e divulgar as regras e servidores aceitos para o envio de mensagens e também critérios para aceitação das mensagens que passaram pelo SPF de outros domínios. Com SPF

o envio de mensagens do tipo *spam* e *phishing* se tornam mais difícil, porque simplesmente os endereços dos remetentes forjados serão bloqueados por servidores que usam SPF ( ZUCCO, 2005 ). Existem várias formas de implementação do protocolo SPF. A seguir será explicado como funciona o chamado “SPF clássico”.

Inicialmente o administrador deve configurar seu DNS para que ele possa divulgar sua política SPF. Devem constar nesta, quais os servidores estão autorizados a enviar e-mail em nome do seu domínio, e também como serão tratadas as consultas feitas para seu domínio.

**Exemplo**:

exemplo.com. IN TXT "v=spf1 a mx ip4:192.168.2.32/27 -all"

No exemplo supracitado a política define que, as mensagens podem ser enviadas em nome do domínio exemplo.com a partir de uma máquina que satisfaça um dos seguintes critérios:

- Endereço IP deve ser um RR tipo A do domínio exemplo.com (a);
- Seja designada como MX do domínio exemplo.com (mx); ou
- Pertença ao bloco de endereços IP 192.168.2.32/27 (ip4).

O argumento "-all" determina que devam ser recusados (prefixo “-“) *e-mails* partindo de qualquer outro endereço IP (all).

Todas as opções de prefixos são:

- "+" *Pass*
- "-" *Fail*
- "~" *SoftFail*

- "?" *Neutral*

O argumento prefixo é opcional, e caso seja omitido o valor utilizado é o "+" (*Pass*).

O argumento "all" define qual será o tipo de resposta retornada da consulta SPF, caso nenhuma das outras cláusulas se aplique.

O administrador de um domínio destinatário que consulte a política do domínio do remetente de email, poderá descartar ou marcar como suspeita uma mensagem que não atenda a política do SPF daquele domínio.

Portanto, a implementação do SPF tem duas partes: domínios devem identificar as máquinas autorizadas a enviar e-mail em seus registros DNS, e os servidores que recebem a mensagem devem requisitar e utilizar as informações SPF, por meio de consultas DNS, que normalmente são armazenadas em cache por questões de performance, e determinar as ações dos e-mails recebidos conforme a tabela de estados listada acima.

SPF não é esperado para eliminar totalmente o *spam/phishing*, mas é mais uma arma na luta contra spam e phishing.

### 2.1.2 Sender ID

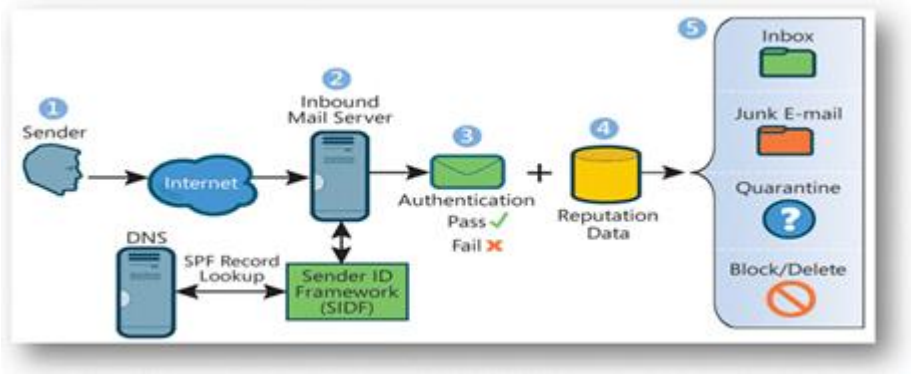
Definido pela RFC 4406 (LYON, 2006) é um protocolo usado pela Microsoft derivado do SPF, onde o campo do endereço da mensagem no cabeçalho, é validado de acordo com RFC 2822 (RESNICK, 2001). Essa validação segue um padrão de algoritmo chamado PRA (*Purported Responsible Address*) especificado na RFC 4407 (LYON, 2006)

O algoritmo verifica se a mensagem partiu realmente do endereço de email que consta do cabeçalho da mensagem. Além de efetuar a validação, o *Sender ID* define nova identidade e PRA além de criar novos campos para política de envio.

*Sender ID* é licenciado pela Microsoft, apesar de ser um projeto de licença pública e precisar da especificação para PRA na entrada TXT do DNS. Por causar alguns erros de sintaxe no padrão SPF, a ferramenta tornou-se pouco implementada.

A ilustração abaixo mostra o funcionamento do padrão Sender ID:

Figura 1: Funcionamento do Sender ID




Fonte: MICROSOFT (2012)

1. O usuário envia uma mensagem de um cliente de e-mail ou interface web. Nenhuma interação ou mudanças para o cliente do remetente ou *Mail Transfer Agent* (MTA) são obrigatórios.

2. O servidor do destinatário de e-mail de entrada recebe a mensagem de e-mail. O servidor usa SIDF e chama o Suposto Responsável pelo Domínio (PRA) DNS para o registro SPF.

3. O MTA receber determina se o endereço IP do servidor de e-mail de saída coincide com os endereços IP que estão autorizados a enviar e-mail para o domínio.

4. Para a maioria dos domínios e IPS, dados de reputação do remetente é aplicada na verificação de veredicto SIDF.

5. Com base na sintaxe registro SPF, a aprovação ou reprovação veredicto, os dados de reputação, e a pontuação de filtragem de conteúdo, o MTA receber envia a mensagem de e-mail para a caixa de entrada, uma pasta de lixo eletrônico ou a granel, ou uma pasta de quarentena. Se uma mensagem de e-mail falhar, a rede receptora pode bloquear, apagar ou *junk* e-mail.

### 2.1.3 DomainKeys

É um sistema *antispam* para verificação do domínio remetente do email e a integridade da mensagem. Apresentado pelo Yahoo! possui função semelhante ao SPF em se tratando da averiguação de mensagens adulteradas, possibilitando rastreamento e comprovação de adulteração com mais facilidade. Foi o grande incentivador para o surgimento de outros protocolos.

O uso da *DomainKeys* oferece duas vantagens:

- Redução do trabalho com tratamento dos abusos de mensagens de seu domínio, caso os destinatários usarem o sistema *DomainKeys* a fim de eliminar automaticamente os emails que se dizem ser desses domínios.
- Focar as forças em ações internas em seus próprios usuários que estejam abusando do domínio.

Ao mesmo tempo, existem incentivos para outros servidores de e-mail habilitarem a verificação do *DomainKey*:

- *DomainKeys* permite identificação da mensagem de origem, permitindo o uso mais efetivo das lista negras ou brancas;

- Ataques *phishing* sejam detectados com maior facilidade;
- E-mails forjados podem ser eliminados automaticamente diretamente no servidor.

Segundo Zucco ( 2005 ), o protocolo DomainKeys funciona realizando um *secure hash* do conteúdo da mensagem (usando o algoritmo SHA-1 por padrão), encriptando o resultado usando uma chave privada (com o algoritmo RSA por padrão) e codificando os dados encriptados com Base64. O resultado dessa operação e adicionado ao e-mail no primeiro campo do cabeçalho SMTP com a chave "*DomainKey-Signature*". Na sua essência, o processo adiciona uma assinatura digital ao e-mail.

O servidor SMTP que recebe a mensagem usa o domínio de origem, ou seja, de onde foi enviado o email e realiza uma nova busca do DNS. A partir dessa consulta o servidor decifra o *hash* do cabeçalho da mensagem e recalcula o valor do *hash* do corpo da mensagem recebida, a partir do ponto imediatamente seguinte ao cabeçalho "*DomainKey-Signature*:". Caso ambos os resultados sejam idênticos, indica-se acerto no local de onde provem a mensagem analisada e que não houve alteração de dados.

*DomainKeys* é compatível com implementações antigas de e-mail, pois utiliza cabeçalhos opcionais SMTP e entradas opcionais TXT no DNS (ZUCCO,2005).

### 2.1.4 DKIM

É uma aprimoração do *Domainkey* e funciona de forma semelhante. No entanto, o DKIM (CROCKER, 2011) possibilita que o dono do domínio publique políticas sugerindo ao servidor de destino uma espécie de direcionamento de ações, como por exemplo, o descarte de todas as mensagens sem devida autenticação.

O site do projeto DKIM (2012), orienta que, para utilizar o DKIM é preciso seguir os seguintes passos:

- Criação de par de chaves pública e privada;
- Disponibilizar a chave publica através do DNS, assim como é feita na publicação da política do SPF;
- Deixar a chave privada no servidor responsável por enviar as mensagens;

Ao enviar a mensagem ela é assinada com a chave privada do servidor. Essa autenticidade é conferida no recebimento da mensagem por meio de averiguação via DNS para obter-se a chave publica e verificar a assinatura (DKIM, 2012).

A partir desta verificação, pode se chegar as seguintes conclusões:

- A assinatura tem validade, ou seja, a mensagem é oriunda do domínio indicado no campo *From.*
- A assinatura não tem validade, indicando mensagem suspeita, passível de descarte;
- Dependendo das políticas locais ou remotas as mensagens não assinadas por um sistema DKIM poderão ou não serem aceitas pelo domínio.

Essa é uma técnica muito promissora que apesar de pouco utilizada se combinada com as técnicas de SPF, podem ser uma ótima ferramenta aliada no combate ao spam e phishing. Esse tipo de ferramenta poderia ser mais utilizada por provedor de acesso, e seus usuários deveriam exigir dessas empresas tecnologias eficientes assim todos contribuiriam para uma internet mais segura e eficiente.

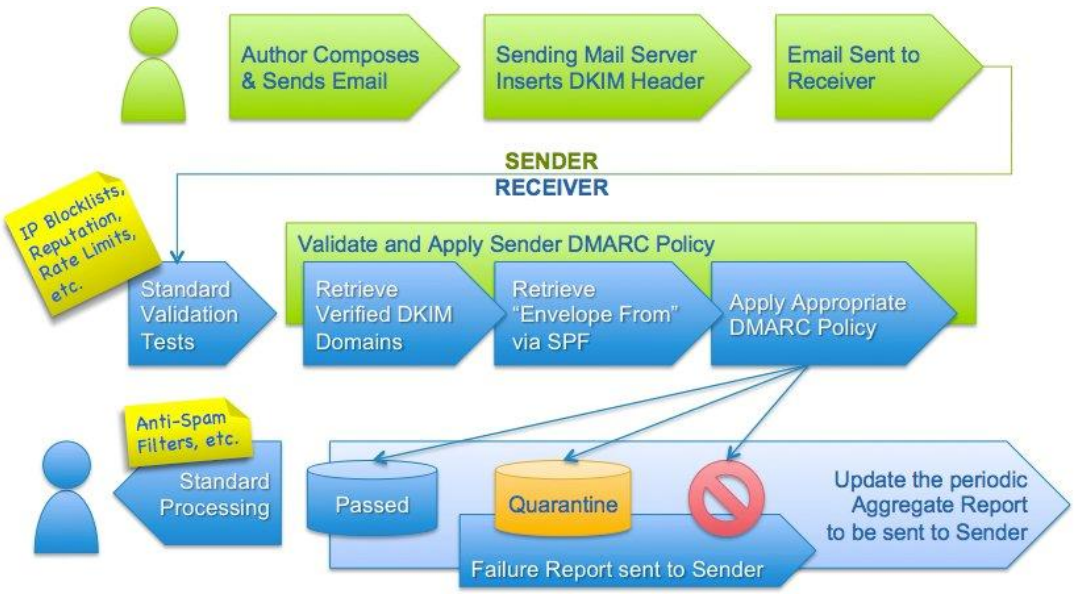
### 2.1.5 DMARC

DMARC (*Domain-based Message Authentication, Reporting & Conformance*) (KUCHERAWY, 2012) que, traduzindo-se significa Relatório e Conformidade de Domínio baseado em Autenticação de Mensagem. Um dos principais objetivos para criação dessa especificação técnica foi a de ajudar pequenas e grandes empresas na redução do abuso sofridos pelo servidores de e-mail no que diz respeito a envio forjados em nome de seus domínios.

O DMARC padroniza como os servidores de destinos irão executar a autenticação de mensagens, fazendo o uso das técnicas SPF e DKIM. O DMARC pretende sanar vários problemas destas duas tecnologias. O principal problema relatado na implantação da tecnologia é a dificuldade na autenticação da maioria das mensagens com SPF ou DKIM, devido à existência de outros serviços de terceiros que acabam impedindo a correta execução das verificações das ferramentas (DMARC, 2012).

Assim, o DMARC baseia-se nesses dois padrões, possibilitando maior controle por parte dos proprietários de domínios, monitorando com mais rigor as mensagens enviadas em seu nome, e gerando um relatório periódico. A figura abaixo ilustra o funcionamento do DMARC.

Figura 2 - Processo de Autenticação de Mensagem - DMARC




Fonte: DMARC (2012)

A especificação permite aos domínios que compartilhem informações entre si. Os destinatários fornecem aos remetentes informações sobre sua forma de autenticação enquanto remetentes dizem o que fazer quando uma mensagem recebida não for autentica (DMARC, 2012).

Segundo o site oficial, a técnica foi desenvolvida objetivando os seguintes requisitos:

- Minimizar os falsos positivos.
- Fornecer relatórios de autenticação robusta.
- Política remetente ao nível de receptores.
- Reduzir a entrega de phishing bem sucedido.
- Trabalhar em escala de Internet.
- Minimizar a complexidade.

Espera-se que a implantação dessa técnica em grandes provedores como AOL, Yahoo!, Hotmail e Gmail estimule outras empresas a adotarem este padrão, contribuindo para

redução na ocorrência de phishing e desta forma tornar a mensagem eletrônica uma forma de comunicação mais confiável.

### 2.1.6 Comparativo entre as Técnicas

**Tabela 4 - Comparativo entre as técnicas**

| | SPF | Sender ID | DKIM |
|---|---|---|---|
| Método de Validação | Endereço do remetente, IP, DNS | PRA, IP, DNS | Assinatura digital do servidor, DNS |
| VANTAGENS | Fácil implementação, Verificação feita antes da chegada dos dados, Proteção contra o problema | Fácil Implementação, verificação feita antes da chegada dos dados, proteção contra o problema de *phishing* | Proteção contra o problema de *phishing*, não e afetado por múltiplos saltos SMTP(*Simple Mail Transfer Protocol*. |
| DESVANTAGENS | Usuários do MTA<br><br>podem forjar identidades de outros usuários, Validação Apenas do ultimo salto | Usuários do MTA podem forjar identidades de outros usuários, validação apenas do ultimo salto | Problemas com reenvio de mensagens, difícil de implementar, problemas de validação de listas de discussão |

**Fonte: ASHIDANI, 2008, p.116**

As técnicas, SPF, Sender ID e DKIM encontram-se demonstradas na tabela 4. Apesar de um grau maior de dificuldade para implantação do DKIM e problemas com validação de listas de discussão, ele demonstra ser juntamente com outras técnicas como o SPF uma forte proteção contra as fraudes envolvendo phishing. (ASHIDANI, 2008).

## 2.2 Como Identificar a Fraude de Phishing

Para o site NIC.BR (2012) , alguns cuidados para são fundamentais na identificação da fraude de *phishing,* dentre os quais destacam-se*:*

- Ler atentamente a mensagem, suspeitando daquelas com muitos erros gramaticais e de ortografia;
- Os fraudadores utilizam técnicas para ofuscar o real *link* para o arquivo malicioso, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Uma sugestão que costuma apresentar êxito é que o usuário deslize o cursor do *mouse* sobre o *link,* desta forma é possível visualizar o real endereço do arquivo na barra de *status*, ou navegador, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- Atenção particular aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões frequentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";
- Mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa devem ser sempre tidas como suspeitas;
- Acesse a página da instituição remetente e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, pode-se observar que não é política da instituição enviar *e-mails* para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.

## 2.3 O que Fazer Com um Caso de Phishing

Segundo o site da CERT.br os incidentes de segurança que envolvam *phishing/scam* devem ser notificados para os responsáveis pela rede que originou a atividade e os responsáveis por hospedar o site fraudulento envolvido. Dessa forma, geralmente a lista de pessoas/entidades a serem notificadas inclui:

- Responsáveis pela rede que originou a atividade;
- Responsáveis por hospedar esquema fraudulento.
- Cert.br

As notificações devem incluir a mensagem identificada como phishing contendo cabeçalho e conteúdo completos. Facilitando dessa forma, o repasse de informações do CERT.BR para os sites lesados para que tomem as devidas providencias, além de contribuir para a manutenção de estatísticas atualizadas do órgão. A notificação poderá ser enviada a qualquer um das entidades abaixo relacionadas:

**CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**

Caso o incidente tenha algum *site* brasileiro envolvidos mantenha o CERT.br informado através do email (cert@cert.br).

**RNP – Rede Nacional de Pesquisa** (RNP, 2012)

Caso você esteja dentro de uma rede participante da instituição de pesquisa ligada a RNP, você pode reportar:

- *Links* maliciosos: artefatos@cais.rnp.br
- Páginas falsas de instituições: phishing@cais.rnp.br

***APWG – Anti-Phishing WorkGroup*** (APWG, 2012b)

- Encaminhar email suspeito para ***reportphishing@apwg.org***

Se estiver com duvida se um site é ou não *phishing* você pode consultar a ferramenta online <http://urlvoid.com/>, que retorna com informação sobre a veracidade do site.

## 2.4 Recomendações de Segurança

A navegação pela internet deve ser feita sempre com cautela e atenção. Nesse tópico vamos abordar algumas recomendações de como os usuário e empresa deve se comportar para terem uma navegação segura e seus dados bem protegidos, seguindo as diretivas do NIC. BR(2010) .

Para usuários:

- Separar os emails para assuntos pessoais, cadastros online, profissionais e compras online. Isso evita receber determinados assuntos indesejados no email do trabalho por exemplo.
- Manter ativo um programa *anti-spam*, ou utilizar o recursos oferecido pelo provedor. Bem como ferramentas de proteção como *firewall*, antivírus, *antispyware*, reduzindo o numero de mensagens indesejadas no email.

Para empresas:

- Adotar estratégias de defesa em camadas.
- Desativar serviços que não são necessários.
- Se algum código malicioso ou alguma outra ameaça explora um ou mais serviços de rede, desabilite ou bloqueie o acesso a esses serviços até que seja aplicado um patch. Isole os computadores infectados.
- Manter os patches atualizados (sistema operacional e aplicações).
- Considerar implementar soluções de acesso e conformidade com políticas de rede.

- Implementar políticas efetivas de senhas e controle de dispositivos.
- Usar softwares de criptografia para proteger as informações.
- Promover treinamento sobre segurança da informação para os funcionários.

O site Internetsegura.org, responsável pelo movimento internet segura, elenca mais algumas ações para uma navegação mais segura:

- Nunca fornecer senha ou informações pessoais – sob nenhum argumento.
- Atentar para barra de endereços – Verifique se o endereço permanece o mesmo durante a navegação. Certificando sempre a existência do cadeado fechado, em endereço iniciados por HTTPS://. Clicando neste cadeado as informações referentes ao certificado são relacionadas ao site em questão.
- Cuidado com promoções tentadoras normalmente recebidas via email, maioria das vezes são encaminhadas por endereços falsos, e prometem descontos e prêmios instantâneos.
- Não navegar e sair "clicando em tudo" - controlar sempre a curiosidade e suspeitar de email que oferecem benefícios de formas fáceis ou por valores muito baixos.
- Emails - Não abrir anexo de desconhecidos ou de conhecidos com erros grotescos de digitação. Abra apenas aqueles dos quais tiver certeza da origem e do possível envio de arquivo anexado.
- Não atestar a veracidade da mensagem apenas pelo remetente que aparece no cabeçalho de um e-mail, pois ela pode ser facilmente forjada pelos atacantes.
- Dados importantes como senhas e números de cartões de crédito, em hipótese alguma devem ser encaminhadas via email.

Para manter-se atualizado, o usuário deve consultar a cartilha do CERT.br (CARTILHA, 2012).

# CAPÍTULO 3 - CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE A SEGURANÇA NA EMPRESA - UMA PROPOSTA.

## 3.1 Cultura de Segurança

Sêmola (2003) menciona que “O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados.” Este é um dos motivos que faz com que o elemento humano seja considerado o elo mais fraco da corrente.

Para que um trabalho de conscientização e mudança de cultura da organização em relação à segurança tenha sucesso, devemos observar os seguintes aspectos:

**Alta Gerência** – Devemos convencer a alta gerencia da importância de se investir na conscientização dos funcionários

**Conscientização** – As pessoas devem estar cientes da necessidade de segurança para os sistemas de informação e redes, assim como o que devem fazer para implementá-la;

**Responsabilidade** – As pessoas são responsáveis pela segurança dos sistemas de informação e redes no seu âmbito de atuação;

**Resposta** – As pessoas devem atuar prontamente e de forma cooperativa para prevenir, detectar e responder aos incidentes de segurança;

**Ética** – As pessoas devem respeitar o interesse legítimo dos outros.

## 3.2 Adoção de Boas Práticas de Segurança

A norma NBR ISO/IEC 17799/2005 estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

A norma serve como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança e para ajudar a criar confiança nas atividades interorganizacionais.

As principais recomendações dessa norma estão detalhadas nas 11 seções abaixo, totalizando 39 categorias principais de SI:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;
- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gerenciamento das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade de Negócios;
- Conformidade.

Tendo como base essa norma podemos destacar alguns itens que merecem atenção no contexto da segurança dos usuários e dos sistemas de correio eletrônico:

***1- Segurança em recursos Humanos - Educação e Treinamento***

Item responsável por assegurar que a força de trabalho entenda suas responsabilidades esteja de acordo com seus papéis

- Assegurar que os funcionários estejam conscientes acerca das ameaças relacionadas à segurança, a responsabilidades e obrigação de cada indivíduo Assim estarão preparados para apoiar a política de segurança e reduzir o risco de erro humano.
- Assegurar que os empregados, fornecedores e terceiros possam deixar a organização de forma organizada.

***2- Gerenciamento das operações e comunicações - Segurança do correio eletrônico***

Item responsável por garantir a operação segura dos recursos de processamento.

- Minimizar o risco de falhas nos sistemas
- Manter a integridade e disponibilidade da informação e dos recursos de processamento.
- Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.
- Prevenir contra a divulgação não autorizada, modificação, remoção ou destruição da informação.
- Manter a segurança na troca informações e softwares internos e externos
- Garantir a segurança do comércio eletrônico
- Detectar atividades não autorizadas de processamento informação

***3-Desenvolvimento de manutenção de sistemas - Uso de assinatura digital***

Visa garantir que a segurança seja parte integrante dos sistemas.

- Prevenir a ocorrência de erros, perdas, modificações não autorizadas ou uso inadequado de informações.
- Proteger a confidencialidade, a autenticidade ou integridade das informações por meios criptográficos.
- Garantir a segurança de arquivos de sistema
- Manter a segurança de sistemas aplicativos e da informação
- Reduzir riscos resultantes da exploração de vulnerabilidades técnicas

Seguir e implementar o uso das boas práticas pode auxiliar a:

- Reduzir o desperdício de recursos de banda, tempo e pessoas e *hardware*.
- Evitar problemas como perda de produtividade e danos à imagem da empresa
- Reduzir perdas financeiras
- Disponibilizar serviços de maior qualidade
- Colaborar para o aumento da segurança da Internet (CERT.br)

## 3.3 Proposta do Programa de Conscientização

Estudos da Universidade de Harvard atribuem ao despreparo do usuário como principal causa de sucesso do *phishing* se relaciona ao despreparo dos usuários, que muitas vezes não conhecem as ferramentas dos navegadores e acabam se deixando levar apenas pelo

aspecto visual. Com isso alguns sites chegam a enganar 90% dos indivíduos, principalmente aqueles que continham gráficos animados, imagens e design moderno. (PAIVA, 2007)

Muito tem se investido em tecnologias que otimizem a detecção de intrusos, firewalls, criptografia e autenticações de fator duplo ou triplo; no entanto se o usuário não estiver conscientizado e preparado adequadamente para agir frente às ameaças, barrar as invasões de sistemas será bastante difícil.

Desta forma, se considerarmos a manipulação dos dados como análoga a uma corrente, podemos constatar que o recurso humano sempre será o elo mais fraco e deve, pois, merecer atenção fundamental, caso se almeje minimizar o sucesso dos ataques *phishing*. No próximo tópico será elaborada uma proposta para implementação de treinamento para usuário acerca da cultura da segurança da informação e os aspectos das técnicas e recomendações para que esses não caiam em golpes e assim contribua para uma organização mais segura.

### 3.3.1 Metodologia de Implantação

A metodologia escolhida para implantação do programa de conscientização foi a adotada pela NBR ISO/IEC 17799/2005, que sugere boas práticas de segurança de TI. Elas são agrupadas em controles relativos dependendo do tipo da situação de risco. Dentre todos os controles da norma, será utilizado como base para execução do programa de treinamento o controle: **Segurança em recursos Humanos - Educação e Treinamento**.

Sobre o controle educação e treinamento, a norma NBR ISO/IEC 17799/2005, enfatiza ainda que é fundamental: "Garantir que os usuários estão cientes das ameaças e das preocupações de segurança da informação e estão equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho".

Por isso os funcionários de uma organização, independente de serem terceirizados ou prestadores de serviços, devem receber treinamento adequado e estarem cientes da preocupação da empresa com a segurança da informação. Devem, portanto, ser orientados e treinados sobre o uso correto dos recursos de TI, reconhecimento de ameaças *phishing*, bem como, receberem atualizações regulares da política corporativa.

Para Ferreira (2008), a implementação de um programa de conscientização na empresa seja eficaz é primordial que haja:

- Planejamento
- Implementação
- Manutenção
- Avaliação periódica

Esse programa geralmente deve seguir as seguintes fases:

1) Identificação do Escopo
2) Identificação dos instrutores
3) Identificação do publico alvo
4) Motivação dos funcionários e da alta administração
5) Administração do programa
6) Continuidade do programa
7) Avaliação do programa

### 3.3.2 Programa de Conscientização

Uma boa e constante iniciativa de conscientização dos usuários, aliada a pesquisa e implementação de novas tecnologias de prevenção e detecção de ataques deve ser

investimento primordial de toda empresa que se preocupa com a questão da segurança da informação. Mas sempre cientes que raramente se estará 100% seguro (BIASOTTO, 2011).

Partindo desse princípio e acreditando que o grande passo para o sucesso das ações *anti-phishing* é a sensibilização dos usuários e a conscientização de sua responsabilidade e importância de seu papel apresentamos uma proposta de programa de conscientização com enfoque no usuário do sistema de informatização da empresa.

1) **Identificação do Escopo**

Explanar sobre a segurança da informação na empresa enfocando as armadilhas que trazem o *phishing*.

Objetivos:

- Conscientizar os funcionários sobre a importância de cada um no controle e na segurança das informações pessoais e empresariais.
- Orientar o usuário a reconhecer as principais formas em que o phishing se apresenta.

2) **Identificação dos instrutores**

Equipe de segurança da informação. Caso não haja, deve ser formada e devidamente treinada previamente.

3) **Identificação do público**

Funcionários da empresa em geral especialmente os que manipulem informações e recursos de TI.

4) **Motivação dos funcionários e da alta direção**

Primeiramente a proposta deve ser apresentada à gerencia e direção da empresa enfocando-se a importância e os benefícios do treinamento para a empresa.

Em relação aos funcionários deverá ser realizado um processo de sensibilização acerca do tema segurança da informação

**Fase 1** - Enviar mensagem aos funcionários alertando acerca da vulnerabilidade dos sistemas de informação.

**Fase 2** – Afixar cartazes informativos abordando as estatísticas e conceitos mais relevantes, de modo conciso, objetivo e direto.

**Fase 3** - divulgação do treinamento e inscrições (via email e presencial).

5) **Administração do Programa**

PROGRAMA DE TREINAMENTO

**Nome:** Programa de Conscientização *Anti-Phishing*.

**Tipo de Abordagem** : Treinamento teórico-prático

**Público-Alvo**: funcionários que de alguma forma manipulem dados de informática

**Duração**: 3 horas

**Metodologia:** O tema será abordado mediante exposição por slides em *Power Point* com recurso de *data-show*, pré e pós-teste, dinâmica de grupo (enfocando o componente "ATENÇÃO" – que é fundamental para o reconhecimento do *phishing*) e avaliação verbal pelos participantes.

Conforme as Orientações para Pré e Pós-teste, da Universidade de Michigan, o pré-teste é definido como um conjunto de perguntas direcionadas aos participantes do evento antes do início da formação, com a finalidade de determinar o grau de conhecimento acerca do conteúdo que será explanado. Ao final da formação, os participantes serão submetidos a

um pós-teste onde serão aplicadas as mesmas perguntas feitas anteriormente, ou perguntas com o mesmo nível de dificuldade

Assim, no primeiro momento do curso realizar-se-á um exercício virtual, disponível no site do OPENDNS (2012), no qual são apresentados algumas páginas de internet verdadeiras  e outras com característica *phishing*, onde o usuário deve apontar qual são os domínios falsos. Ao fim da tarefa será realizado um *print screen* em cada máquina o qual será utilizado em confronto com o pós teste a realizado ao fim do curso.

**Programação**

1. Pré-teste (15 minutos)
2. Parte 1 (50 minutos)
    a. Introdução ao phishing - Segurança TI
    b. Alguns conceitos básicos phishing/ Estatística
    c. Reconhecendo a ameaça / Prejuízo para empresa
3. Intervalo: Coffee Break (15 minutos )
4. Vitalizador (dinâmica)  (15 minutos)
5. Parte 2 (60 minutos)
    a. Exemplos mais comuns de phishing
    b. Boas práticas para utilização dos recursos de TI
    c. Apresentação da política de segurança e normas internas
6. Pós Teste (15 minutos)
7. Avaliação da formação. (10 minutos)

6) **Continuação**

O programa será revisado sempre que houver publicação de novas normas internas e será reavaliado anualmente de acordo com novas tendências de tecnologias no tema segurança da informação.

7) **Avaliação**

**Curto prazo**: a princípio será realizada uma avaliação baseada no cruzamento de dados obtidos no pré e pós teste onde será mensurado a porcentagem de acertos sobre reconhecimento de *phishing*. Também será levada em conta a avaliação verbal feita pelos participantes ao fim da formação teórico pratica. Essas informações auxiliarão os facilitadores a perceberem o grau de assimilação do conteúdo ministrado e se por ventura haverá necessidade de algum ajuste bem como avaliar se a metodologia aplicada obteve o alcance satisfatório de sucesso ou necessita de adequações.

**Longo prazo**: será avaliado mediante estatísticas internas da empresa em relação à invasão de phishing e outras ameaças virtuais no ambiente TI da empresa.

## CONSIDERAÇÕES FINAIS

O referido estudo nos levou a refletir sobre a parcela de culpa que as empresas tem tido, quando negligenciam uma formação de base para seus recursos humanos. Outrossim, não basta que uma organização tenha políticas de segurança, normas de acesso, tecnologia de ponta, se um dos grandes pilares ainda permanece “fraco”.

Baseado nesse entendimento decidiu-se realizar este trabalho dando enfoque ao elemento “usuário”. E diante disso, destacamos como aspectos positivos a disponibilidade de novas ferramentas no mercado no combate ao phishing, como exemplo do padrão DMARC, que chega para corrigir falhas de outros padrões e prima por minimizar o recebimento de mensagens fraudulentas e indesejadas.

Acredito que esse estudo pode ser útil para auxiliar equipes de suporte em segurança da informação a reconhecerem a importância ímpar de se preparar os recursos humanos, sejam eles funcionários ou usuários domiciliares. A aplicação do exemplo proposto é perfeitamente viável e com grandes chances de sucesso por ser simples, objetivo, financeiramente acessível, dependendo mais de fatores organizacionais como equipe especializada e treinada para ministrar a formação, bem como, aceitação por parte da diretoria da empresa.

**REFERÊNCIAS**

ABNT. NBR ISO/IEC 17799:2005. Tecnologia da informação: Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

APWG. Activity Trends Report. Disponível em: <http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf>. Acesso em: jul. 2012.

APWG. Anti-Phishing WorkGroup. Disponivel em: < http://www.antiphishing.org>. Acesso em: jul. 2012b.

ASHIDANI, Pedro Junior et al. Proposta de framework para autenticação de remetente. In: THE THIRD INTERNACIONAL CONFEREN OF FORENSIC COMPUTER SCIENCES, 1, Rio de Janeiro, 2008. Rio de Janeiro, Brasil, 2008, 111-116 pp.

BIASOTTO, Abner. Os usuários de sua empresa dão munição para ataques de SPEAR PHISHING?, 2011. Disponível em: <http://www.tiespecialistas.com.br/2012/04/os-usuarios-de-sua-empresa-dao-municao-para-ataques-de-spear-phishing-?/>. Acesso em 21 jun. 2012.

BRAGA, PH. Técnicas de Engenharia social. Universidade Federal do Rio de Janeiro, 2010. Disponível em: <http://www.gris.dcc.ufrj.br/documentos>. Acesso em 08 jun. 2012.

CARTILHA. Cartilha de Segurança para Internet. Disponível em: <http://cartilha.cert.br> Acesso em: jun. 2012.

CERT.br. Incidentes Reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/2012-apr-jun/analise.html>. Acesso em: jul. 2012.

COMPUTERWORLD. Spams causam prejuízos de bilhões de dólares para empresas. Disponível em: <http://computerworld.uol.com.br/seguranca/2011/11/09/spams-causam-prejuizos-de-bilhoes-de-dolares-para-empresas/ > Acesso em: jul. 2012.

CROCKER, D et al. DomainKeys Identified Mail (DKIM) Signatures. Disponível em < http://www.ietf.org/rfc/rfc6376.txt>. Acesso em: julho/2012. 2011

DKIM. DomainKeys Identified Mail- Service Overview. Disponível em: < http://dkim.org/specs/rfc5585.html>. Acesso em: jun. 2012

DMARC. DMARC Overview. Disponível em: <http://www.dmarc.org/overview.html > Acesso em: jun. 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu. Política de segurança da Informação: Guia Prático para Elaboração e Implementação. 2ª Edição Revisada: Editora Ciência Moderna, 2008.

JUNIOR, MG; LIMA, SM. Segurança e confiabilidade em sistemas de informação: dois lados da mesma moeda. In Revista Eletrônica da faculdade adventista de administração do Nordeste – FAAD 2010.

LAUDON, Kenneth C.; LAUDON, Jane P. *Sistemas de informação gerenciais*. Thelma Guimarães (trad.). Ed 7. São Paulo: Pearson Prentice Hall, 2007.

LYON, J. RFC 4406 - Sender ID: Authenticating E-Mail. Disponível em <http://www.ietf.org/rfc/rfc4406.txt>. Acesso em: julho/2012.

LYON, J. RFC 4407 - Purported Responsible Address in E-Mail Messages. Disponível em <http://www.ietf.org/rfc/rfc4407.txt>. Acesso em: julho/2012.

KUCHERAWY, M. Domain-based Message Authentication, Reporting and Conformance (DMARC). Disponível em < http://www.dmarc.org/draft-dmarc-base-00-02.txt>. Acesso em: julho/2012.

MARTINS, Diego de Oliveira. *Phishing Scam: A fraude do Século 21*, 40 f. Universidade Federal do Rio de Janeiro, 2008.

MICROSOFT. Sender ID Framework Overview: Verification System Aims to Reduce Spam and Increase Safety Online. Disponível em:<http://www.microsoft.com/mscorp/safety/technologies/senderid/overview.mspx>. Acesso: 20 jul. 2012.

MOVIMENTO INTERNET SEGURA. Práticas para evitar fraudes na internet. Disponível em: <http://www.internetsegura.org/dicas/seguranca_mandamentos_dicas.asp> Acesso em: mar. 2012.

NIC.BR – Núcleo de Informação e Coordenação do ponto BR. Disponível em: <http://www.antispam.br>. Acesso em: jun. 2012.

NIU,Y et al. Iphishing: Phishing, Vulnerabilities on Costumer Eletronics. University of California, Davis, 2008. Disponível em:<http://www.usenix.org/.../niu_html>. Acesso em 02 jun. 2012.

OLIVEIRA, Márcia C. ; VIEIRA, Alexandre T. Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas. Universidade Luterada do Brasil. ( ULBRA), Canoas, RS, 2011.

OLIVO, CK. *Avaliação de características para detecção de phishing de email.* Dissertação(mestrado), Pontifícia Universidade Católica do Paraná, Curitiba, 2010.

ORIENTAÇÕES para pré e pós teste: Guião de implementação técnica #2, University of Michigan 2008. Disponível em <http://www.go2itech.org/.../2tig_pre_pos_teste_a4.pdf> Acesso em 28 jul. 2012.

OPENDNS. Think you can outsmart Internet scammers?. Disponível em: <www.opendns.com/phishing-quiz> Acesso em: jun 2012.

PAIVA, Cláudio. Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil, 2007. Disponível em: <http://www.alfa-redi.org/node/8970> Acesso em 25 jun. 2012

RESNICK, P. RFC 2844 - **Internet Message Format**. Disponível em <http://www.ietf.org/rfc/rfc2822.txt>. Acesso em: julho/2012.

RNP. Rede Nacional de Ensino e Pesquisa. Disponível em <http://www.rnp.br>. Acesso em: jul. 2012.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma visão executiva. Rio de Janeiro: Campus, 2003.

SILVA, Ricardo costa. Gestão estratégica da tecnologia instrumentos teóricos e aplicações. Vol II. Feira de Santana , Radami, 2008.

SYMANTEC. Relatório da Symantec constata que pequenas empresas são alvo de quase um terço dos ataques mundiais direcionados, 2012. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20120710_01> Acesso em 28 jul. de 2012

UNIESP. Um novo e caro hobby da internet, 2011. Disponível em: <http://www.administraçãouniesp.files.wordpress.com/2011/05/um_novo_e_caro_hobby_da_internet.pdf>. Acesso em 6 jun. 2012

URLVOID. Security Tools for Webmaster. Disponível em: <http://urlvoid.com>. Acesso em: jun 2012

ZUCCO, Jeronimo Cleberson. *Técnicas e Ferramentas de Código Aberto Para Combate ao Spam*, 90 f. Projeto de Diplomação(Graduação)- Universidade de Caxias do Sul, 2005.

WONG,M ; SCHLITT, W. **Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1.** Disponível em < http://www.ietf.org/rfc/rfc4408.txt>. Acesso em: julho/2012.