https://www.ctir.gov.br

01 de janeiro de 2019

Recomendação nº 01/2019
Golpe de Phishing

Atualização: 14 de junho de 2019

Por favor, entre em contato com o **CTIR Gov**, caso tenha alguma dúvida relacionada a esta publicação, por meio dos contatos a seguir.

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-2315

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

Obs.: As informações aqui disponibilizadas têm o objetivo de fornecer avisos e recomendações sobre questões comuns de segurança da informação para integrantes de órgãos e entidades de governo e para o público em geral.

Dentro das trocas de informações entre CSIRTs, esta publicação está marcada como **TLP:WHITE***. Sujeitas às regras padrão de direitos autorais, as informações do TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**).

1. Descrição do Problema

Atacantes vêm concentrando esforços na exploração de vulnerabilidades dos usuários, uma vez que é mais complexo atacar ou fraudar com sucesso um servidor (ativo computacional) de uma instituição. Esses atacantes, aqui tratados como golpistas ou fraudadores, se utilizam de técnicas de engenharia social e por diferentes meios e discursos, procuram enganar e persuadir potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas. Existe vasta gama de golpes na *Internet*, esta recomendação se dedica a tratar da fraude definida como ***Phishing***.

Phishing, ***phishing scam*** ou ***phishing-scam***, é o tipo de fraude, por meio da qual, um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social levando a vítima a divulgar informações ou clicar em um *link* malicioso. O ***phishing*** pode ser realizado por meio de uma mensagem de texto, mídia social ou por telefone, mas atualmente a maioria das pessoas usa o termo para descrever ataques que chegam por *e-mail,* que vem a ser um método de entrega ideal para ataques dessa natureza, pois pode atingir os diretamente o usuário e se esconder entre o grande número de *e-mails* benignos recebidos.

O **CTIR Gov** recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, da presente recomendação, orientando como as organizações podem se defender contra *e-mails* maliciosos que usam técnicas de engenharia social.

2. Impacto

Este tipo de fraude pode ocasionar a suas vítimas: extravio e divulgação de informações sensíveis; destruição de informações; indisponibilidade de serviços computacionais comprometidos; furto de identidade; prejuízo financeiro; e danos à imagem.

3. Dispositivos Afetados

Ainda que a utilização de ferramentas *antiphishings* ou *antimalwares* previna ou mitigue parte considerável desses golpes, alguns deles chegam às vítimas sem serem detectadas. Isso ocorre porque muitas vezes as mensagens maliciosas são enviadas de remetentes conhecidos (que podem
ter sido invadidos ou forjados) ou ainda por se utilizarem quase que exclusivamente o ataque de engenharia social para persuadir as vítimas.
O ambiente computacional é meio para o ataque de engenharia social. Por esse motivo os mais diversos dispositivos podem ser afetados.

4. Recomendações

Elementos típicos encontrados nessas mensagens podem ajudar a caracterizá-las:

- ✓ são mensagens que chamam a atenção, apresentando-se como originária de instituições familiares ao usuário (seus bancos, Serasa, Receita Federal, etc.);
- ✓ persuadem o usuário de da necessidade de recadastro de senha, atualizações de software, recebimento de prêmio ou vantagem financeira, etc.;
- ✓ solicita dados pessoais, tais como *login* e senha, dados bancários, número de CPF, telefone e endereço, o que normalmente instituições não solicitam via *e-mail*;
- ✓ a mensagem possui tom de urgência, ligada a ameaças de bloqueio, suspensão de serviços, etc.;
- ✓ solicitações de cliques em *links*, o que deve sempre servir de fonte de suspeita. Tais *links* servem para redirecionar o usuário para um site malicioso, com páginas imitando o formato e arte de instituições legítimas. Uma armadilha comum é a existência de um *link* com a promessa de não se receber mais outro tratando do assunto citado no atual;
- ✓ ocorrências de erros ortográficos, por vezes grosseiros, que também podem indicar que o texto original foi traduzido por meio de algum aplicativo;
- ✓ a mensagem pode abordar assuntos relacionados a eventos atuais ou épocas específicas, como os relativos ao envio do Imposto de Renda, enviados pela Receita Federal; e
- ✓ Alguns exemplos que ajudam a identificação de mensagens fraudulentas, podem ser encontrados no site **Catálogo de Fraudes da RNP** (*https://catalogodefraudes.rnp.br/*), disponibilizado pelo **Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS/RNP)**, que também serve como fonte de informação para o auxílio a não propagação de fraudes disseminadas por *e-mail,* bem como na prevenção desse tipo de golpe.

4.1 Prevenção

4.1.1. O melhor princípio de prevenção é o uso de bom senso. O autor do golpe tenta se utilizar das emoções da vítima, tentando atrair sua atenção, provocando curiosidade, oferecendo vantagem financeira e instigando urgência.

4.1.2. Exemplos de ações de prevenção ao golpe:

- ✓ nunca confiar plenamente remetente e seu endereço, constantes na mensagem de *e-mail*. Essa informação pode ser modificada para ocultar um endereço falso;
- ✓ em mensagens falsas, é comum o remetente e o endereço de resposta serem diferentes;
- ✓ em caso de dúvida, entrar em contato com a pessoa ou organização que supostamente enviou a mensagem e confirmar o seu envio e as informações que ela possui.
- ✓ existem formas variadas de *phishing*. técnicas semelhantes podem ser utilizadas também por telefone, *chat*, SMS, mensagens de texto, etc.;
- ✓ Atenção a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;
- ✓ questionar o motivo de instituições, com as quais não se tenha relacionamento, estarem enviando mensagens, como se houvesse alguma relação prévia (exemplo: não ter conta em determinado banco, não existindo motivo de se recadastrar dados ou atualizar módulos de segurança);
- ✓ ficar atento a mensagens que apelem demasiadamente pela atenção do usuário e que, de alguma forma, o ameace caso não execute os procedimentos descritos;
- ✓ não considerar que uma mensagem é confiável com base na confiança que se deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
- ✓ ser cuidadoso ao acessar *links*. Procurar digitar o endereço diretamente no navegador *Web*;
- ✓ verificar o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o ***phishing***. Ao posicionar o mouse sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- ✓ utilizar, e manter atualizados, mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing*;
- ✓ verificar se a página utiliza conexão segura. Sites de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;
- ✓ verificar as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao site verdadeiro; e
- ✓ acessar a página da instituição que supostamente enviou a mensagem e procurar por informações (não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

4.2 Mitigação

4.2.1. Em caso de suspeita de recebimento de ***phishing*** ou comprometimento de credenciais, notifique imediatamente a equipe de tratamento de incidentes computacionais, setor de segurança ou suporte de tecnologia da informação da sua organização. No caso de não possuir o contato da equipe de segurança de seu órgão, notifique o **CTIR Gov**, endereço *ctir@ctir.gov.br* .

4.2.2. Para a correta execução da notificação, deve ser encaminhada a mensagem, não deixando de incluir o conteúdo do cabeçalho de *Internet* completo da mensagem suspeita de ser maliciosa.

4.2.3. O cabeçalho de *Internet* de um *e-mail* é a parte da mensagem que tem as informações do remetente, assunto, data e destinatário, entre outras informações. Na leitura normal de uma mensagem, apenas algumas informações estão à mostra, justamente aquelas colocadas pelo programa utilizado pelo remetente, não confiáveis, pois podem ser forjadas.

4.2.4. O cabeçalho de *Internet* completo, oferece mais informações importantes para determinar seus dados corretos de origem, inclusive caminho percorrido. Confira abaixo a forma de obter corretamente o cabeçalho completo da mensagem, dependendo de como as mensagens são lidas:

- ✓ ***Outlook para o Office 365, 2016, 2013 ou 2010 em um PC***
  - Clique duas vezes em uma mensagem de email para abri-lo fora do painel de leitura.
  - Clique em "*Arquivo*" > "*Propriedades*".
  - Informações de cabeçalho aparecem na caixa "*cabeçalhos de Internet*".
  - Pressione **Ctrl + C** para copiar.
- ✓ ***Outlook 2007***
  - Abra a mensagem de email.
  - Na guia "*mensagem*", no grupo "*Opções*", clique no "*Iniciador de caixa de diálogo*".
  - Na caixa de diálogo "*Opções de Mensagem*", os cabeçalhos são exibidos na caixa "*Cabeçalhos de Internet*".
  - Pressione **Ctrl + C** para copiar.

- ✓ ***Outlook Express***
  - Abra o ***Outlook Express***.
  - Clique com o botão direito do *mouse* no *e-mail* do qual você deseja ver o cabeçalho.
  - Clique em "*Propriedades"*.
  - Clique na guia "*Detalhes"*.
  - O cabeçalho será mostrado na caixa exibida.

- ✓ ***Hotmail***
  - Faça *login* na sua conta do ***Hotmail***.
  - Clique em "*Entrada*".
  - Clique com o botão direito do *mouse* no *e-mail* do qual você deseja ver o cabeçalho.
  - Clique em "*View Message Source"*.
  - O cabeçalho aparecerá em uma nova janela.
- ✓ ***Gmail***
  - Abra o ***Gmail*** em um navegador.
  - Abra o *e-mail* cujo cabeçalho você quer verificar.
  - Ao lado de "*Responder*", clique na seta para baixo.
  - Clique em "*Mostrar original*".
  - O cabeçalho aparecerá em uma nova janela, que mostrará os resultados da autenticação. Para ver o cabeçalho completo da mensagem, copie tudo abaixo de "*Fazer download da mensagem original*".
- ✓ ***Inbox by Gmail***
  - Abra o ***Inbox*** em um navegador.
  - Abra o *e-mail* cujo cabeçalho você quer ver.
  - Na mensagem, clique em "*Mais*" > "*Mostrar original*".
  - O cabeçalho aparecerá em uma nova janela.
- ✓ ***Yahoo! Mail***
  - Faça *login* na sua conta do ***Yahoo! Mail***.
  - Selecione o *e-mail* cujo cabeçalho você quer ver.
  - Clique em "*More*" > "*View Raw Message*".
  - O cabeçalho aparecerá em uma nova janela.
- ✓ ***Apple Mail***
  - Abra o ***Apple Mail***.
  - Abra o *e-mail* cujo cabeçalho você quer ver.
  - Clique em "*View*" > "*Message*" > "*All Headers*".
  - O cabeçalho aparecerá na janela abaixo da Caixa de entrada.
- ✓ ***Mozilla***
  - Abra o ***Mozilla***.
  - Abra o *e-mail* cujo cabeçalho você quer ver.
  - Clique em "*View*" > "*Message Source*".
  - O cabeçalho aparecerá em uma nova janela.
- ✓ ***Opera***
  - Abra o ***Opera***.
  - Clique no *e-mail* do qual você deseja ver o cabeçalho para que ele seja exibido na janela abaixo da Caixa de entrada.
  - Clique com o botão direito do *mouse* no corpo do *e-mail*.
  - Clique em "*View All Headers and Message*".
  - O cabeçalho aparecerá na janela abaixo.
- ✓ ***AOL***
  - Faça login na sua conta da AOL.
  - Abra o *e-mail* cujo cabeçalho você quer ver.
  - No menu "Action", selecione "*View Message Source"*.
  - O cabeçalho aparecerá em uma nova janela.

4.2.5. Para ver mais detalhes de como obter o cabeçalho de Internet de sua mensagem de e-mail, bem como de outros gerenciadores de e-mail em: ***How to Get Email Headers*** (*https://mxtoolbox.com/Public/Content/EmailHeaders/*).

5. Referências

- Catálogo de Fraudes da RNP - Disponível em: *https://catalogodefraudes.rnp.br/*. Acesso em: 24 de mar 2019.
- Cartilha de Segurança para *Internet* - Disponível em: *https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf*. Acesso em: 24 de mar 2019.
- Mensagens Fraudulentas – *phishing* - Disponível em: *http://www.ufrgs.br/tri/Documentos/mensagens-fraudulentas-phishing*. Acesso em: 24 de mar 2019.
- *Phishing Attacks: Defending Your Organisation* - Disponível em: *https://www.cpni.gov.uk/system/files/documents/63/b4/Phishing_Attacks_Defending_Your_Organisation.pdf*. Acesso em: 24 de mar 2019.
- Exibir cabeçalhos de mensagem de internet - Disponível em: *https://support.office.com/pt-br/article/exibir-cabe%C3%A7alhos-de-mensagem-de-internet-cd039382-dc6e-4264-ac74-c048563d212c*. Acesso em: 24 de mar 2019.
- Rastrear um e-mail pelo cabeçalho completo - Disponível em: *https://support.google.com/mail/answer/29436?hl=pt-BR*. Acesso em: 24 de mar 2019.
- *How to Get Email Headers* - Disponível em: *https://mxtoolbox.com/Public/Content/EmailHeaders/*. Acesso em: 24 de mar 2019.
- **PADRÕES PARA NOTIFICAÇÃO DE INCIDENTES AO CTIR Gov**. (*https://www.ctir.gov.br/arquivos/publicacoes/Padronizacao_Notificacao_CTIRGov.pdf*)

Coordenação-Geral do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR)

Informações: cgtir@presidencia.gov.br
Notificação de incidentes: ctir@ctir.gov.br