BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 21– Outubro/2021

Recomendações para o uso de aplicativos e serviços de mensagens instantâneas

O uso de aplicativos e serviços de mensagens instantâneas facilita a comunicação casual e organizacional, trazendo mais agilidade para o dia a dia, disponibilizando recursos como chamada de voz, envio de imagem, vídeo, áudio e texto. É necessário saber quão seguros são esses meios de comunicação - o que cada aplicativo desenvolve e apresenta, a fim de garantir a segurança das informações ali trocadas e também o que pode-se fazer para não correr riscos.

Alguns cuidados, de maneira geral, devem ser observados:

- ✓ verifique se o aplicativo utilizado tem a criptografia de ponta a ponta. Ela garante que os dados permaneçam seguros e privados até chegarem ao seu destino;

Curiosidade: utilizar um teclado GIF ou realizar backup das mensagens, compromete a criptografia ponta a ponta.

- ✓ apague suas conversas regularmente;
- ✓ limite a visibilidade das suas informações apenas para os seus contatos;
- ✓ utilize o recurso de autenticação de dois fatores;
- ✓ mantenha a segurança do seu dispositivo por meio de telas de bloqueio e alteração frequente das senhas;

E, caso o seu órgão ou entidade utilize o serviço de mensagem instantânea para fins de atividades laborais, recomendamos que:

- em caso de incidente de segurança da informação, ameaça cibernética ou vulnerabilidade do aplicativo, os administradores de grupo adotem as medidas aplicáveis e avisem imediatamente ao Gestor de Segurança da Informação de seu órgão ou entidade;
- as conversas privadas e de grupos, cujo o objetivo já tenha sido esgotado e que não precisem ser mantidos por razões administravas ou legais, sejam apagadas periodicamente;
- os administradores de grupos devem ter ciência das responsabilidades administrativas e legais as quais estão sujeitos quanto à moderação de conteúdo; e
- o uso do aplicativo de mensagens deve estar em conformidade com a Política de Segurança da Informação e as normas correlatas do órgão ou da entidade.

Hacker

A palavra *hacker* vem do termo inglês *hack*, que significa cortar alguma coisa de forma grosseira ou irregular. É geralmente associada a programadores de sistemas, que utilizam seus conhecimentos para cometer crimes.

Na verdade, trata-se de um especialista em ciência da computação, dotado de conhecimentos e habilidades que permitem a ele conhecer aspectos vulneráveis ou negligenciados pelos desenvolvedores de um determinado sistema.

Existem *hackers* que utilizam seu conhecimento tanto para o bem, quanto para o mal. A sua atuação varia de acordo com as motivações que ele nutre.

Os "*hackers* do mal" tem como prática a quebra ilegal de segurança de um sistema, *site*, servidor etc, com o objetivo de proveito pessoal, financeiro ou não, caracterizando crime.

Para evitar ser hackeado, siga as dicas abaixo:

- use uma senha exclusiva para cada conta;
- não clique em anúncios ou *links* estranhos;
- procure por *sites* com a extensão HTTPS no endereço;
- não use computadores públicos para fins pessoais;
- tenha e mantenha atualizado um programa de antivírus; e
- use autenticação de dois fatores sempre que puder.

Se você for vítima de um *hack* de segurança, denuncie o golpe ou evento de invasão imediatamente. Você pode ajudar a reduzir o dano, além de evitar que outras pessoas se tornem vítimas.

Você conhece quais são as **responsabilidades do Gestor de Segurança e Credenciamento**?

Cabe ao Gestor de Segurança e Credenciamento (GSC):

- a manutenção da qualificação técnica necessária à segurança de informação classificada no seu órgão público;
- a implantação, controle e funcionamento dos protocolos de documentos classificados;
- a conformidade e o sigilo dos processos de credenciamento e habilitação no âmbito do seu órgão público;
- a proposição à Alta Administração de normas para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restrito no seu órgão público;
- a gestão dos recursos criptográficos, das Credenciais de Segurança e dos materiais de acesso restrito;
- o assessoramento da Alta Administração do seu órgão público para o tratamento de informações classificadas.

A competência do GSC está regulada pelo artigo 17 da Instrução Normativa nº 02 do GSI/PR.

Para saber mais informações sobre esse assunto ou outras acesse: https://www.gov.br/gsi/dsi/

BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 21– Outubro/2021

ATENÇÃO!

Você conhece a fraude digital chamada de *Pharming*?

Pharming é um golpe *on-line* por meio do qual atacantes instalam um código malicioso em seu computador ou em um servidor da rede, que irá redirecionar seu navegador automaticamente para *sites* falsos. O objetivo, como sempre, é coletar informações pessoais, como dados de cartão de pagamento ou senhas de bancos, *e-mails* etc.

A definição de *pharming* no dicionário é a prática de criar ou cultivar animais ou plantas geneticamente modificadas para desenvolver produtos farmacêuticos. No mundo cibernético, o termo *pharming* é um neologismo baseado nas palavras *phishing* (que lembra *fishing*, termo em inglês que significa "pescaria") e *Farming* (termo em inglês que significa agricultura), remetendo à ideia de que o *hacker* conseguirá atingir muitos usuários de uma vez só com este ataque, ao invés de um a um como acontece no *phishing*. Este abuso também é conhecido como "*Phishing* sem isca". Você vai entender melhor na continuação do texto.

Enquanto o conhecido *Phishing* utiliza *links* em *e-mails* fraudulentos para induzir um clique e o acesso a *um website* falso, o *Pharming*, por outro lado, consiste em um processo de duas etapas:

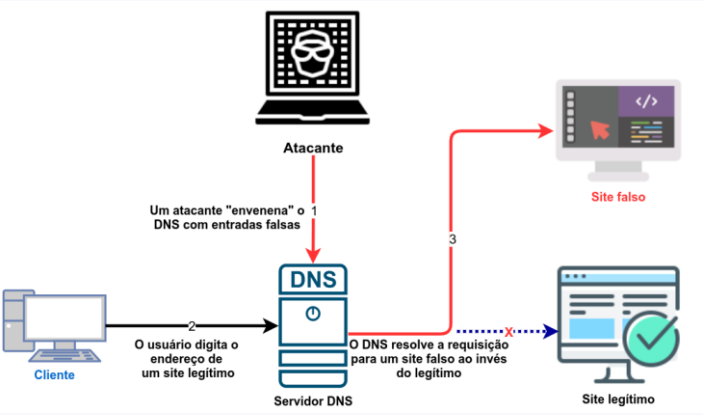
1º - o atacante instala um código malicioso no alvo, que pode ser um computador ou em um servidor da rede, neste caso, todos os usuários que fizerem uso desse servidor, correrão o risco de sofrer fraude;

2º - quando o usuário digitar um *link* legítimo (de um banco, por exemplo), o navegador irá redirecionar o acesso para um *site* fraudulento, onde o fraudador terá acesso imediato a qualquer informação ali inserida.

Este golpe envolve o abuso de um sistema chamado de DNS (*Domain Name System*), que traduz os nomes dos *sites* que você digita no navegador em endereços IP na *Internet*. Assim, em uma situação normal, seu navegador *web* se conecta ao servidor do *site* desejado com o devido endereço IP.

Entretanto, se este serviço DNS for indevidamente alterado, o acesso a um endereço legítimo pode direcionar o tráfego de seu computador, não, para o devido endereço IP, mas para um endereço IP ilegítimo. Quando isso ocorre, dizemos que a tabela DNS está envenenada e o computador está sendo vítima de um ataque de *Pharming*.

A figura abaixo ilustra como ocorre este ataque.



Fique atento a duas dicas importantes para desconfiar de um ataque de *Pharming*:

1. Um *site* que sempre utiliza https (conexão segura), de repente passa a apresentar apenas http na barra de endereços - isso é um indício de que o *site* pode ter sido clonado; e
2. Um *site* que parece estranho, com alguns erros de ortografia, fontes diferentes das que você está acostumado, ou com falhas inesperadas em seu desenho - isso é um forte indício de que algo não está certo.

As principais dicas para se manter seguro são:

- altere a senha padrão em seus roteadores e pontos de acesso *wireless;*
- habilite a autenticação de dois fatores sempre que possível;
- verifique sempre se você está usando conexões seguras https;
- mantenha sempre seu Sistema Operacional e os programas antivírus atualizados;
- tenha cuidado ao abrir *links* ou anexos que você não esperava, ou que são de um remetente desconhecido; e
- não acesse *sites* suspeitos e de conteúdo claramente ilícito (seu navegador normalmente apresenta alertas).

Se você suspeitar que está sendo vítima de um ataque de *Pharming* em sua organização, avise imediatamente seu Administrador de Rede. Se o problema for em sua residência, verifique em seu computador e roteador quais são as entradas de DNS e entre em contato com provedor de serviços de *Internet* para se certificar das devidas configurações.

Fonte: https://www.gov.br/gsi/dsi/ https://www.ctir.gov.br/

Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br