TORREÃO BRAZ
ADVOGADOS

Brasília, 18 de setembro de 2017.

COMUNICADO

Assunto: Fraudes perpetradas por meio de e-mails, mensagens de texto (SMS) e mensagens por Whatsapp

Na atualidade, é muito comum a comunicação por meio de dispositivos eletrônicos: enviamos e recebemos diversas mensagens de texto (SMS, WhatsApp), utilizamos e-mail, Skype etc.

Esses meios de comunicação são excelentes e facilitam muito o nosso dia a dia, mas também podem ser terreno fértil para pessoas mal intencionadas, que se utilizam deles para praticarem todo tipo de "golpes".

Como esses "golpes" estão se tornando cada vez mais frequentes, elaboramos o presente comunicado, no qual daremos exemplos dos principais tipos de fraudes praticadas por meio de dispositivos eletrônicos, bem como dicas de como se proteger delas.

1) **Como as fraudes são praticadas**

Os fraudadores geralmente almejam receber alguma quantia em dinheiro ou conseguir a informação que dará acesso a uma de suas contas bancárias (como a data e o local de seu nascimento, o nome de seus pais etc.). Para conseguir essas informações, eles geralmente se utilizam de mensagens de texto, por celular ou e-mail. Essa prática é chamada de *phishing*.

O assunto e o conteúdo das mensagens geralmente será convidativo ou alarmante: o saque de uma quantia em dinheiro sem seu cartão de crédito; o bloqueio do cartão; a troca da senha do cartão e/ou do banco; a confirmação de uma compra que você não fez; um prêmio que você ganhou etc.

As mensagens virão acompanhadas de algum comando, como: clique no *link* para saber onde foi feito o seu saque sem cartão; recadastre a sua senha de cartão clicando no seguinte *link;* baixe o anexo e informe-se sobre o boleto etc.

Esses *links* e anexos podem possuir vírus ou ser portas de entrada de crackers (pessoas maliciosas que querem invadir o seu computador e roubar suas informações).

2) **Dicas de como se proteger das fraudes**

– Nunca abra um link ou anexo de mensagem suspeita ou não solicitada;

– Suspeite de mensagens que pedem informações pessoais e/ou confidenciais (como senhas, datas de nascimento; perguntas de segurança etc.);

– Suspeite de mensagens intimidadoras e não ceda à pressão para o envio de suas informações;

– Sempre confira o remetente. Os fraudadores podem cometer erros de grafia ou mudar detalhes no endereço de e-mail (exemplo: remetente governamental que não utiliza o final ".gov");

– Desconfie de mensagens que informem que você ganhou algum prêmio. As empresas raramente entram em contato dessa forma.

Essas dicas não são infalíveis, mas certamente são úteis para aumentar a sua segurança na internet.

Seguem, abaixo, *links* de sítios eletrônicos, em que constam outras informações acerca das mencionadas fraudes:

https://www.rnp.br/servicos/seguranca/catalogo-fraudes

https://br.norton.com/phishing-tips/article

https://support.apple.com/pt-br/HT204759

http://www.techtudo.com.br/noticias/2017/05/golpe-de-phishing-tenta-roubar-apple-id-de-iphone-veja-como-funciona.ghtml

http://www.techtudo.com.br/noticias/noticia/2015/04/seguranca-no-celular-identifique-golpe-phishing-no-e-mail-e-mensagens.html

http://pt.wikihow.com/Detectar-um-E%E2%80%90mail-de-Fraude-ou-Phishing