Para não morder a isca

Como se proteger do phishing, prática criminosa que consiste no roubo de dados online

Atire a primeira pedra quem nunca recebeu um e-mail do banco alertando para o cancelamento da conta, caso não seja realizada uma atualização dos dados cadastrais pelo link disponibilizado na mensagem. Trata-se do phishing, uma das formas mais comuns de roubo de dados. A novidade é que o tal e-mail agora pode vir também na forma de uma mensagem de WhatsApp, um SMS ou uma ligação telefônica. “As mensagens normalmente têm algum apelo emocional, para induzir a pessoa a clicar no link malicioso e fornecer seus dados”, explica o presidente da Comissão de Segurança da Informação (Comsi), Cláudio Felipe Magioli. No contexto da segurança da informação, esse tipo de ataque envolvendo manipulação psicológica é conhecido como engenharia social.

O e-mail continua sendo o principal meio de perpetuação do golpe, mas já há danos causados também pelo smishing, quando a mensagem fraudulenta é enviada por SMS. “Como o uso de smartphones só cresce, esse tipo de ataque acaba sendo tão efetivo quanto o e-mail”, explica o assessor de Segurança da Informação do TRE-RJ, Frederico Guerra, que tratou do assunto na 117ª edição do Parlatório. Segundo especialistas em segurança da informação, vem crescendo também o uso de aplicativos de troca de mensagens, como o WhatsApp, para a aplicação desse tipo de golpe.

“Em tempos de fake news, é muito provável que ataques de phishing via WhatsApp tenham sucesso”, alerta Cláudio. Ele explica que, pelo aplicativo, o link malicioso pode vir disfarçado. Por exemplo, na forma de uma URL encurtada. Além disso, tem uma capacidade de disseminação muito rápida, através dos compartilhamentos. Outro método utilizado para os ataques é o vishing, em que o criminoso explora a confiança da população nos serviços de telefonia para persuadir as vítimas a fornecer números de cartão de crédito, senhas e outros dados que serão posteriormente usados em golpes de roubo de identidade. “As chamadas por VoIP (voz sobre IP) também são utilizadas para os ciberataques”, conta o presidente da Comsi.

Conhecimento é a melhor defesa

“Utilizar filtros que bloqueiem mensagens indesejadas, manter antivírus e firewalls atualizados são medidas importantes, mas a principal defesa contra os ataques é manter-se informado sobre as técnicas mais recentes de phishing”, ensina Frederico. Para Cláudio, o conhecimento também é a melhor defesa. “Os cibercriminosos vêm sofisticando suas técnicas. Muitas vezes nos protegemos contra um ataque e outros cinco novos aparecem”, conta. Formulado pelo Tribunal Regional Federal da 3ª Região (TRF3) e obrigatório para todos os servidores da Justiça Eleitoral fluminense, o curso de segurança da informação foi uma das medidas adotadas pelo TRE-RJ para evitar ataques a seus colaboradores.

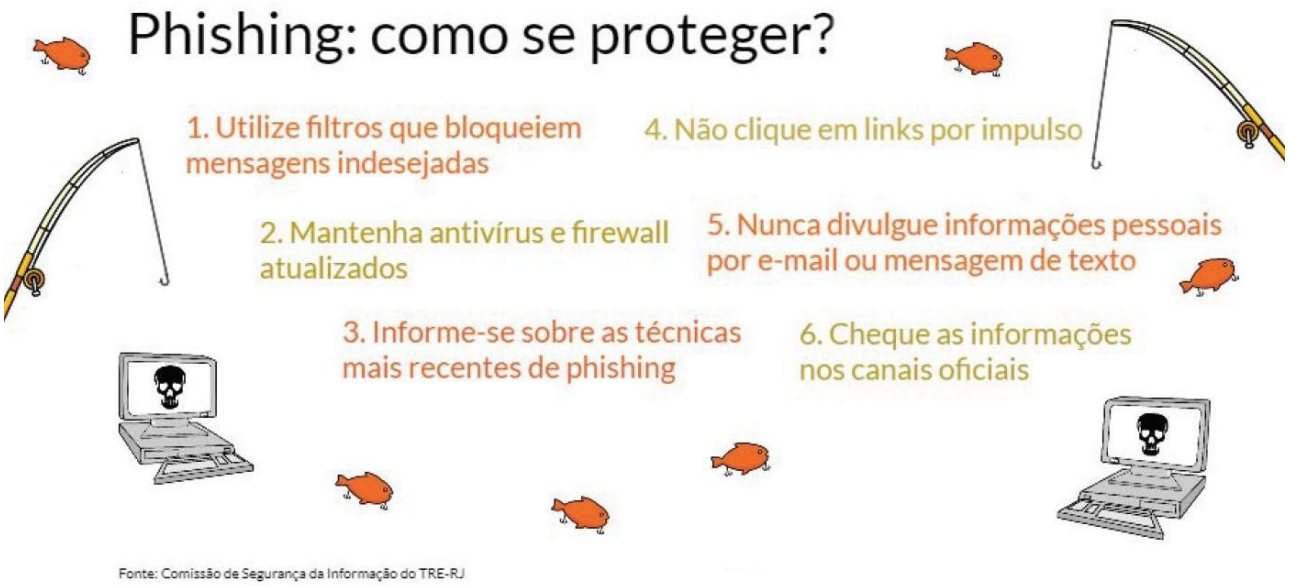
“Apesar de haver ataques a redes, as pessoas são o elemento mais vulnerável na segurança da informação”, assegura Frederico. Por isso, outra dica dos especialistas é pensar antes de clicar. “Devemos ler as mensagens que recebemos com um olhar crítico e checar as informações com fontes confiáveis antes de clicarmos nos links fornecidos. Além disso, devemos sempre verificar a segurança dos sites visitados”, sugere Cláudio. Outra dica é sempre pesquisar se aquela instituição costuma entrar em contato com seus clientes e quais os canais oficiais utilizados. “Por exemplo, o TRE-RJ não costuma enviar e-mails ou mensagens aos eleitores. No entanto, esse tipo de criminoso poderia se aproveitar do prazo final da biometria obrigatória para aplicar golpes, mandando

mensagens em nome do Tribunal", explica Frederico.

Os dois servidores concordam que a principal forma de prevenção é nunca divulgar informações pessoais. "Precisamos entender que não devemos fornecer dados pessoais ou financeiros, por meio de links fornecidos, e-mails ou mensagens de texto", alerta Cláudio. Ele sugere que, ao receber uma mensagem que solicite dados pessoais, o cidadão entre em contato com a instituição pelo site oficial ou telefone, para confirmar a informação recebida. "Não é preciso viver com medo de ataques de phishing, basta seguir algumas normas de segurança para aproveitar uma experiência online sem preocupações", afirma o assessor Frederico.

Foto: Tatiana Grossi

FOCO NAS PESSOAS
A equipe da Comsi reúne-se periodicamente para traçar estratégias de proteção de dados mais focadas nas pessoas, que são o elemento mais vulnerável na segurança da informação



Fonte: Comissão de Segurança da Informação do TRE-RJ