30/12/2012 - McAfee adverte consumidores sobre os 12 golpes on-line de Natal para este ano

Cibercriminosos aproveitam a época das festas de fim de ano para desenvolver novos ataques e fraudes virtuais

Anualmente, a McAfee realiza um levantamento sobre as compras on-line para as festas de Natal. Para este ano, a empresa de segurança digital investigou os hábitos, comportamentos, interesses e estilos de vida dos consumidores norte-americanos que indicam que a Internet e os dispositivos móveis são os meios preferidos das pessoas para fazer compras nesse período. A partir disso, a McAfee também identificou os 12 principais golpes que estão sendo usados mundialmente pelos cibercriminosos para roubar a identidade e as informações bancárias dos consumidores globais.
A pesquisa revelou que os norte-americanos têm usado cada vez mais dispositivos móveis para atividades diárias, pois 70% dos entrevistados disseram planejar fazer compras pela Internet e, desse total, um em cada quatro afirmou que usará seu smartphone para essa finalidade. Apesar de 87% dos consumidores contatados terem se mostrado preocupados com a possibilidade de roubo de informações pessoais durante o uso de um aplicativo em aparelhos móveis, nove em cada dez usuários estão dispostos a fornecer dados pessoais para receberem ofertas que lhes sejam vantajosas.
O levantamento da McAfee apontou ainda que 88% dos norte-americanos que planejam fazer compras pela Internet para as festas de 2012 utilizarão um computador pessoal, enquanto 34% usarão um tablet e 19%, um smartphone. Como mais da metade dos consumidores acessará aplicativos para fazer compras ou acessar sites de bancos e cerca de 30% dos usuários de dispositivos móveis nos Estados Unidos admitem não prestar atenção a todas as permissões de aplicativos, esses equipamentos se tornaram alvo dos golpistas com o uso de aplicativos mal-intencionados, tendo o objetivo de roubar dados pessoais e informações bancárias.

A McAfee relaciona a seguir os 12 golpes mais perigosos na Internet e que devem ser evitados:

1) Lojas virtuais falsas – sites falsos de comércio eletrônico, que parecem ser reais, tentam induzir o consumidor a digitar seu número de cartão de crédito e outros dados pessoais. Após obter os dados do usuário, o consumidor jamais receberá a mercadoria e suas informações pessoais permanecerão em risco par uso indevido do cibercriminoso.

2) Aplicativos móveis mal-intencionados – os usuários de dispositivos Android baixaram mais de 25 bilhões de aplicativos[i]. Com o aumento da popularidade desses programas, também aumentam as chances de que o consumidor baixe um aplicativo mal-intencionado projetado para roubar informações ou distribuir mensagens de texto pagas sem o seu conhecimento.

3) Golpes de viagens – antes de reservar um voo ou hotel para viajar nessa época, o consumidor não deve se esquecer de que os golpistas querem atraí-lo com preços abaixo do mercado. Páginas da Web de agências de viagens falsas são usadas para induzir o fornecimento de dados financeiros.

4) Spam/phishing de Natal – muitos dos emails de spam apresentam temas natalinos. Relógios Rolex e produtos farmacêuticos baratos, por exemplo, podem ser anunciados como “o presente perfeito” para pessoas especiais. Atenção às ofertas boas demais para serem verdadeiras!

5) iPhone 5, iPad e outros golpes com presentes de Natal atraentes – o entusiasmo causado por equipamentos eletrônicos de última geração são a isca preferida dos cibercriminosos quando planejam seus golpes. Eles divulgam os presentes de Natal obrigatórios em links perigosos, concursos falsos e emails de phishing como forma de atrair a atenção dos consumidores e fazer com que eles revelem informações pessoais ou cliquem em links perigosos, que podem baixar malwares para suas máquinas e dispositivos.

6) As mensagens de Skype – o Skype é bastante utilizado para contatar amigos e parentes na época de Natal. Entretanto, os usuários devem estar cientes do novo golpe de mensagens do Skype, que infecta as máquinas. Muitas vezes, esses programas maliciosos sequestram arquivos e, para tê-lo de volta, o usuário é obrigado a pagar um resgate.

7) Cartões e Vales-presentes falsos – os cibercriminosos oferecem, ainda, cartões de presente falsos na Internet. É preciso ter cuidado ao comprar vales-presentes de terceiros, pois eles podem ser uma fraude.

8) SMiShing de Natal – SMiSishing é a prática de phishing por meio de mensagens de texto em dispositivo móvel. Assim como nos emails de phishing, o golpista tenta induzir o usuário a

revelar informações, fingindo ser uma empresa legítima.

9) Golpes de redes e mídias sociais – muitos internautas usam sites de rede social para conversar com a família e os amigos na época de Natal. Por saber que os usuários confiam em seus contatos, os cibercriminosos usam esses canais para anunciar concursos falsos e ofertas de trabalho em casa. Os golpistas também podem tentar invadir contas do Facebook e do Twitter para distribuir alertas falsos a todos os amigos do usuário.

10) Instituições beneficentes falsas – este é um dos maiores golpes a cada temporada de festas. Os golpistas aproveitam as doações usuais a instituições beneficentes e enviam emails de spam com publicidade de instituições falsas.

11) Cartões virtuais perigosos – os cartões virtuais são uma maneira popular de enviar um agradecimento rápido ou desejar Boas Festas, mas alguns são mal-intencionados e podem conter spyware ou vírus que são baixados no computador ou dispositivo quando o usuário clica no link para ver a mensagem.

12) Classificados falsos – os sites de classificados na Internet podem ser um ótimo lugar para procurar presentes de Natal, mas é preciso ter cuidado com ofertas falsas que pedem muitas informações pessoais ou que seja transferida uma quantia em dinheiro, pois pode tratar-se de um golpe ou fraude.

“A melhor maneira de os usuários se protegerem é conhecer os truques dos cibercriminosos para evitá-los. Os consumidores não podem baixar a guarda para os ataques virtuais durante o Natal", ressalta José Matias Neto, diretor de Suporte Técnico da McAfee para a América Latina.

O executivo dá algumas dicas sobre como se proteger contra os golpes das festas de fim de ano:

1) Desconfie sempre – os consumidores devem desconfiar de qualquer oferta que pareça ser boa demais e sempre procurar indicações de que um email ou site possa não ser legítimo,

como imagens em baixa resolução, erros ortográficos, erros de gramática ou links estranhos.

2) Pratique a navegação segura – para descobrir se um site pode conter ameaças ao computador ou dispositivo, antes de clicar nele, instale um plug-in de pesquisa segura, como o McAfee SiteAdvisor®
. O SiteAdvisor usa ícones de verificação nas cores vermelha, amarela e verde para avaliar os sites no momento em que o consumidor realiza a busca, alertando-o para o risco ou não em acessar o site indicado na pesquisa.

3) Compre com segurança – quando realizar compras online, sempre utilize sites respeitados e procure um selo que indique que a segurança do site foi verificada por um fornecedor externo confiável, como Marcão selo de confiança McAfee SECURE™. Além disso, procure um símbolo de cadeado e verifique se consta a letra “s” “https” no início do endereço do site (em vez de apenas “http”), para verificar se o portal usa criptografia para proteger seus dados.

4) Use senhas de alta segurança – as senhas devem ter pelo menos oito caracteres e conter uma variedade de letras, números e caracteres especiais que não formem palavras. Evite usar a mesma senha para suas contas importantes e nunca as revele a ninguém. Crie uma senha forte!

5) Tenha cuidado ao clicar – não clique em links que aparecem em mensagens de pessoas desconhecidas e, caso você se depare com uma URL abreviada, use um expansor de URL para saber o destino do link antes de clicar nele.

6) Use uma proteção abrangente no computador e dispositivos móveis – os consumidores precisam de uma proteção completa, que inclua antivírus, antispyware, antispam e um firewall. Verifique se essa proteção está atualizada. Soluções como a recém-lançada linha de suítes de segurança McAfee® 2013 e da solução completa McAfee® All Access auxiliam na segurança dos consumidores e de seus familiares. Especificamente o McAfee All Acces efetua a proteção de todos os dispositivos do consumidor – PCs, Macs, smartphones e tablets – contra malwares, phishing, spyware e outras ameaças comuns e emergentes, a partir de uma única solução a preço acessível.

7) Informe-se – mantenha-se atualizado sobre os últimos golpes e truques aplicados pelos

cibercriminosos, hackers e fraudadores e evite possíveis ataques. O consumidor pode encontrar mais informações e dicas úteis no Centro de Informações de Segurança da McAfee (página em português).

Para obter informações sobre as ameaças mais recentes, além de checar dicas sobre como navegar com segurança, os internautas podem visitar o Centro de Orientação Informações de Segurança da McAfee e a página da McAfee no Facebook em www.facebook.com/mcafee

Sobre a McAfee
A McAfee, uma subsidiária pertencente à Intel Corporation (NASDAQ:INTC), permite às empresas privadas, ao setor público e aos usuários domésticos aproveitarem com segurança os benefícios da Internet. A empresa oferece soluções e serviços de segurança proativos e comprovados para sistemas, redes e dispositivos móveis em todo o mundo. Com sua estratégia Security Connected, uma inovadora abordagem de segurança aprimorada por hardware, e a exclusiva rede Global Threat Intelligence, a McAfee dedica-se ininterruptamente a manter seus clientes em segurança. http://www.mcafee.com/br

Ketchum – assessoria de imprensa da McAfee no Brasil