Prezado usuário,

Toda instituição é vítima de ataques virtuais, ou seja, pessoas de fora tentam entrar em sua rede de computadores para obter os mais variados tipos de informação possíveis. Tudo depende da intenção: alguns querem apenas se divertir e outros querem utilizar o que for descoberto em benefício próprio – invariavelmente de forma ilegal.

Com a rede da FDE e SEESP a situação não é diferente e várias tentativas acontecem todo dia.

É verdade que temos um sistema bastante estruturado de proteção, entretanto alguns ataques acabam tendo sucesso porque contam com a possível distração dos usuários. Sem querer ou sem saber, muitos de nós, acabamos por fornecer informações que depois podem ser utilizadas de forma inadequada.

As duas formas mais comuns pelas quais podemos fornecer essas informações sem querer são **respondendo à um e-mail falso** ou **preenchendo um formulário numa página da Internet**. O e-mail geralmente tem uma carga apelativa e oferece um link que deve ser clicado; o formulário aparece durante a navegação na Internet, geralmente a partir de um chamariz (um anúncio, uma foto) que tem um link que leva a uma página na qual o usuário precisa dar informações em troca do "benefício".

A equipe de especialistas em segurança da DTI/*GSTIC - Gerência de Suporte de Tecnologias da Informação e Comunicação* nos oferecerem algumas dicas de como podemos proteger nossas informações e as da Fundação. Confira a seguir:

Nunca devemos fornecer senhas e nem dados pessoais (endereço, número de documentos etc.) para resolver problemas financeiros ou legais

Não importa o argumento do e-mail que foi enviado – "sua conta bancária precisa de atualizações", "seu nome está no SERASA", "você caiu na malha fina do Imposto de Renda" – não devemos fornecer senhas e informações pessoais pela Internet. As grandes instituições bancárias, comerciais e governamentais se utilizam de outros recursos para resolver os problemas com as pessoas físicas. Elas sabem que e-mail é algo que pode facilmente ser fraudado.

Negócios imperdíveis, sorteios e ofertas tentadoras

Não importa o apelo – "clique aqui e ganhe uma viagem para Nova Iorque", "você acabou de ser sorteado", "seus sonhos serão realizados em um clique" – bons negócios não são propostos à distância e grandes promoções não são ofertadas a um número restrito de pessoas apenas por e-mail, principalmente o que é utilizado no trabalho. Devemos desconfiar quando a oferta é demais.

Ajuda humanitária

Algumas fraudes se utilizam da disposição de algumas pessoas em ajudar o próximo. Não devemos fazer doações e nem fornecer informações ao receber e-mails ou abrir páginas que fazem pedidos de caráter beneficente. As instituições idôneas se utilizam de outros meios.

Toda atenção à barra de endereços do navegador da Internet

Quando navegamos pela Internet, o endereço fica visível no navegador (veja abaixo). Se ao clicar num link o endereço mudar para algo que não tenha relação nenhuma com aquilo em que estamos navegando, a melhor atitude é fechar o navegador e esquecer o site.

Muito cuidado ao fazer pagamentos pela Internet

Diversas fraudes acontecem quando as pessoas vão fazer pagamentos pela Internet. É preciso saber muito bem para quem estamos passando permissão para movimentar nossa conta bancária. Além de perder dinheiro, podemos abrir as portas para os fraudadores utilizarem nossos dados de forma ilegal ou criminosos invadirem a nossa rede.

E-mails de pessoas desconhecidas

Todos os profissionais, escolas e órgãos ligados à FDE, à SEE e ao Governo do Estado tem e-mails terminados em **gov.br** (ex: usuário@fde.sp.gov.br, usuário@educacao.sp.gov.br etc.). Os colaboradores de fora da FDE – por exemplo, os fornecedores – também têm e-mail padrão da empresa de que fazem parte. Não devemos abrir links que estejam em e-mails de pessoas que não conhecemos.

E-mails de caráter pessoal no ambiente de trabalho e assuntos bombásticos

É fácil desconfiar que o e-mail não é relacionado ao trabalho pelo próprio assunto e características. Muitas mensagens que vêm com notícias de última hora sobre celebridades, catástrofes, barbáries ou com a famosa mensagem “clique aqui para ver as imagens” são uma armadilha e, ao clicar nelas, a pessoa pode acabar descarregando, em seu micro ou na rede, um vírus ou algo do gênero. Se o e-mail não tem nenhum tema de interesse profissional, o melhor a fazer é descartá-lo.

Evidentemente há muitos outros modos de prevenir os ataques, mas esses são os principais. Caso você tenha curiosidade sobre esse tipo de assunto, recomendamos a leitura do Manual do Comitê Gestor da Internet no Brasil – http://internetsegura.fde.sp.gov.br/Arquivos/cartilha-seguranca-internet.pdf.