Dicas de Segurança para Suas Comunicações

As seguintes práticas de segurança estão sendo oferecidas apenas como referência, e recomendamos aos leitores que consultem seus departamentos de Segurança da Informação para instruções específicas.

As ameaças de segurança cibernética afetam as pessoas de modo regular, em seus dispositivos corporativos e pessoais, e é necessário um nível superior de segurança e consciência no uso de ambos os dispositivos. Como é cada vez mais comum que os empregados participem em programas corporativos de Bring Your Own Device (traga seu próprio dispositivo), a linha entre comunicações pessoais e corporativas é cada vez mais tênue, já que, com frequência a informação da empresa é acessada através de dispositivos pessoais. A seguinte lista de melhores práticas pode ajudá-lo a reduzir riscos.

Em Dispositivos Pessoais:

- **Certifique-se de acessar a informação da empresa utilizando apenas ferramentas de segurança implementadas por sua organização.** Evite utilizar webmail ou conectar-se à rede corporativa sem uma conexão segura. Não armazene informação corporativa sensível em dispositivos pessoais. Sempre que possível dê prioridade à separação entre recursos utilizados para o trabalho e para assuntos pessoais;
- **Evite o uso de conexões Wi-Fi gratuitas e públicas.** Se isto for inevitável, considere o uso de uma solução VPN em seu computador pessoal e em seu celular pessoal, para impedir a captura de seus dados;
- **Antes de clicar em qualquer link ou ao abrir arquivos anexos tente realizar uma inspeção dos mesmos.** Se quaisquer dos seguintes elementos não forem os habituais, não clique no link ou abra o anexo: horário de envio, variações mínimas no endereço de e-mail, nome do arquivo, ou mesmo o endereço da rede do link, incluída no e-mail. Se clicar em um link suspeito ou no arquivo anexo, não utilize seu dispositivo até executar um detector de vírus, e realize todas as recomendações necessárias de limpeza;
- **Siga periodicamente os seguintes passos para garantir que seus dispositivos pessoais estejam seguros:**
  - Atualize o sistema operacional de seu celular/laptop sempre que solicitado pelo sistema;
  - Certifique-se de utilizar um navegador de internet atualizado;

- Preste atenção aos alertas de pop-up quando estiver navegando, e não admita exceções de segurança, especialmente para certificados vencidos ou para ignorar notificações ou advertências de segurança;
- Os laptops devem incluir uma solução antivírus, que seja atualizado periodicamente;
- Tenha certeza que uma criptografia (HTTPS na barra de endereços) está em uso ao inserir qualquer nome de usuário e senhas; se você não tem certeza de que a criptografia está sendo usada pela aplicação, utilize um servidor VPN reconhecido.

- **Todos os dispositivos devem ser protegidos por uma senha complexa e exclusiva.** Enquanto estiver em viagem, tente manter seus dispositivos portáteis pessoais junto a você ou a um colega. Evite deixar seus dispositivos em quartos de hotéis e cofres. Enquanto estiver em viagem ao exterior, evite autorizar atualizações do sistema, já que estas podem ser alertas fraudulentos enviados ao conectar-se a um serviço de Wi-Fi do hotel;
- **Verifique e comprove a legitimidade de todos os aplicativos que deseja instalar em seu dispositivo pessoal.** Aplicativos mal-intencionados circulam amplamente e podem capturar tudo que for digitado em seu teclado e ainda informação armazenada em seu dispositivo.

Sobre as Redes Sociais:

- Modifique as senhas de forma periódica e certifique-se de que as mesmas não estejam duplicadas em diferentes redes sociais ou em outras plataformas sensíveis, tais como contas corporativas, contas bancárias e contas de e-mails pessoais;
- Habilite a autenticação de múltiplos fatores, se esta estiver disponível. Esta ferramenta é frequentemente oferecida nas redes sociais mais conhecidas; no entanto, o usuário deve optar por ativá-la. Esta pode ser encontrada no menu de ajuda ou na opção de busca;
- Esteja atento às solicitações de conexão por parte dos usuários, mesmo daqueles com conexões já estabelecidas com familiares e amigos dentro de sua rede. Os fraudadores estão sempre online, fazendo-se passar como contatos legítimos;
- Mantenha-se familiarizado com os filtros e as regras de privacidade para estar consciente de como os conteúdos são compartilhados. Frequentemente, as redes sociais realizam mudanças, solicitando atenção periódica do usuário quanto às suas configurações. Estabeleça filtros de privacidade nos mais altos níveis;
- Seja cauteloso ao clicar em um link enviado por e-mail, especialmente nas URLs abreviadas, quando estiver conectado a uma dessas redes sociais. Este é o principal mecanismo usado para infectar um dispositivo com malware. Para acessar o site, abra uma nova aba no navegador e escreva o nome do site na barra de endereços; não copie e cole a URL;
- Evite clicar em qualquer link dentro de e-mails ao abrir arquivos anexos que você não estiver esperando, principalmente quando os e-mails estiverem marcados com o logotipo de redes sociais. Ao invés disso, acesse essas redes sociais diretamente através da URL. A qualidade dos sites falsos torna difícil a distinção destes dos reais, enganando os usuários, que fornecem informações pessoais ao clicar em um link para conectar-se com o site falso.

1461575 08/16