Dicas de Segurança para Internet no Trabalho

1 Proteja seu computador

Mantenha todos os softwares atualizados (incluindo seu navegador da Web) com atualizações automáticas, e instale todas as atualizações de segurança que seu departamento de TI recomenda. Use softwares antivírus, anti-spam e anti-spyware e ative seu firewall.

2 Pense antes de compartilhar informações confidenciais

- Busque por sinais de que uma página da Web é segura, antes de inserir informações pessoais confidenciais ou dados corporativos – um endereço da Web com https ("s" de seguro) e um cadeado fechado ( ) ao seu lado.
- Nunca envie informações confidenciais em resposta a e-mails ou mensagens instantâneas (MI).

3 Pense antes de clicar

- Faça uma pausa antes de abrir anexos ou clicar em links de e-mails ou mensagens instantâneas, mesmo que você conheça o remetente; eles podem ser falsos. Confirme com o remetente se a mensagem é verdadeira, ou visite o site oficial digitando você mesmo o endereço.
- Seja cuidadoso ao clicar em links ou botões em janelas de pop-up.

4 Use senhas fortes

- Proteja contas online, o computador, o telefone e outros dispositivos com senhas de no mínimo oito caracteres (quanto maiores, melhor) e inclua letras maiúsculas e minúsculas, números e símbolos.
- Mantenha senhas e PINs em segredo. Não revele-as para colegas de trabalho ou empresas (como um operador de cybercafé), e não seja enganado divulgando-as sem querer.
- Não use a mesma senha para tudo.

5 Proteja-se contra golpes por e-mail

- Tome cuidado com mensagens alarmistas, palavras com a grafia errada ou erros gramaticais, propostas que parecem boas demais para ser verdade, pedidos de informações confidenciais como número de contas e outros sinais de golpes. Ative um filtro que o previna contra sites suspeitos.

6 Proteja seus dados mesmo fora de casa ou do escritório

- Ao usar uma rede Wi-Fi pública, escolha a opção mais segura, mesmo se tiver de pagar por ela. Ela pode incluir uma proteção com senha e criptografia.
- Confirme a grafia exata da rede sem fio que você está se conectando. Fique atento com cópias "espertas" (com o nome escrito de maneira levemente diferente).
- Criptografe os dados em seu laptop (ou unidade flash USB), para o caso de perdê-lo ou ele ser roubado.
- Guarde seu laptop, smartphone e PDA tão cuidadosamente quanto sua carteira.

Mais Esperto Online = Mais Protegido Online

O Que Fazer Caso Haja Problemas

Ao usar um serviço da Web

Ao usar e-mails, redes sociais ou outro serviço, você pode se deparar com golpes, material obsceno e comportamento agressivo, ou ainda roubo de sua conta ou identidade.

- Relate ao serviço. Por exemplo, em nos serviços ou softwares Microsoft®, procure pelo link **Relatar Abuso**, ou mande um e-mail para **abuse@microsoft.com**.
- Relate qualquer representação inapropriada de sua organização ao seu departamento de TI – por exemplo, um golpe de phishing com um e-mail se passando por sua empresa.

Roubo ou perda de informações corporativas confidenciais

Se dados de clientes, ou qualquer outro tipo de dados confidenciais foram comprometidos por roubo ou perda de laptop, smartphone ou outro dispositivo móvel, ou por alguma falha na segurança de rede:

- Informe imediatamente ao departamento de TI e de segurança da empresa.
- Mude todas as senhas utilizadas para o logon no dispositivo.
- Para smartphones e PDAs, entre em contato com o provedor do serviço para ajudá-lo a apagar os dados do dispositivo.

Mais Informações Úteis

- Se você administra uma empresa sem suporte de TI, a Microsoft pode ajudá-lo a defender melhor os computadores da empresa: **microsoft.com/brasil/seguranca**.
- Busque por informações completas a respeito de como ajudar a proteger seu computador, e sua privacidade, em **microsoft.com/brasil/proteja**.
- Para obter informações sobre os produtos de infraestrutura da Microsoft, acesse **microsoft.com/brasil/servidores**.
- Se o seu computador não está funcionando conforme o esperado (está lento demais ou falha frequentemente), ele pode ter sido danificado por softwares mal-intencionados, como um vírus ou spyware. A Microsoft pode ajudá-lo a resolver isso. Para mais detalhes acesse **safety.live.com**.
- Aprenda mais sobre como proteger sua família em: **www.navegueprotegido.com.br**.