Guia de Segurança Online

A Internet trouxe enormes benefícios, que vão desde permitir que as pessoas se comuniquem, façam compras e transações bancárias on-line até facilitar o comércio internacional entre as empresas. Infelizmente, no entanto, é também um terreno fértil para criminosos que procuram meios e oportunidades para que:

- Infectem o seu computador, celular ou tablet com malware e roubem a sua identidade;
- Enviem e-mails fraudulentos e de spam;
- Enganem você fazendo com que visite sites falsos e entregue suas informações pessoais;
- Entrem em sua rede sem fio e interceptem os seus dados, como senhas e nomes de usuários;
- Assumam o controle do seu computador e o utilizem para atacar computadores de outras pessoas.

Proteja-se Online

Existem alguns passos simples que você pode seguir para se proteger on-line, seja você o proprietário de uma empresa ou um indivíduo particular. Sempre há mais coisas que você pode fazer, mas sugerimos que você siga no mínimo as diretrizes abaixo.

Dicas de Senha

Ao criar senhas, lembre-se do seguinte:

- As suas senhas são secretas e somente você deve possuir acesso. Ninguém do HSBC jamais pedirá a você a sua senha de internet banking ou de plataformas HSBC;
- Torne-as difíceis de adivinhar;
- Varie. Procure utilizar senhas diferentes para diferentes serviços;
- Mude suas senhas regularmente;
- Nunca as anote.

Computador Protegido

Mantenha o seu sistema operacional, navegadores da web e outros softwares atualizados. A cada momento são descobertas novas vulnerabilidades em programas e aplicativos de computador. Essas vulnerabilidades podem ser exploradas por criadores de vírus e hackers para obter acesso a computadores.

A fim de corrigir essas vulnerabilidades, os desenvolvedores de software lançam regularmente os patches de segurança. Certifique-se de que seu navegador e sistema operacional estejam configurados para atualizar automaticamente para que não perca patches de segurança importantes. Os novos softwares normalmente vêm com essa configuração, verifique nos manuais de instalação.

Você também pode verificar se há novos patches e fazer atualizações visitando o site do fabricante, normalmente na seção "Download". Geralmente, as versões mais recentes de sistemas operacionais (como o Microsoft Windows) ou navegador (como o Internet Explorer, o Google Chrome, o Apple Safari e etc.) possuem os recursos de segurança mais atualizados. Os usuários Microsoft podem atualizar o Windows

clicando em “Todos os Programas” no menu “Iniciar” de seus computadores e então selecionar a opção “Atualizar Windows”.

Os usuários Apple Mac podem verificar se há atualizações de software clicando em Atualizações na barra da App Store ou selecionando Atualização de Software no Menu Apple. Ou então, visite o site https://www.apple.com/downloads.

Desconfie de e-mails falsos sobre falsas atualizações. Utilize o software de atualização que vem junto com o seu computador ou o próprio site do editor de software – não clique em links fornecidos por e-mails.

Instale um Software de Antivírus

O software de antivírus protege você, sua privacidade e o seu dinheiro.

Os vírus são nocivos, pois roubam informações pessoais, controlam o seu PC, exibem anúncios indesejados e podem até mesmo usar o seu computador para atacar os computadores de outras pessoas. Eles também podem ser chamados de malware, cavalos de troia, ransomware, spyware ou adware. O software de antivírus protege você contra todos eles.

Para que possa funcionar corretamente, o software de antivírus precisa estar devidamente atualizado. Um software de antivírus desatualizado apresentará falhas e vulnerabilidades.

Qualquer arquivo sem extensão (um que seja nomeado simplesmente como "file", por exemplo) ou com uma extensão dupla (file.wow.jpg, por exemplo) é possivelmente um vírus e nunca deve ser aberto. Além disso, nunca abra um anexo de e-mail desconhecido e, em especial, um que contenha um arquivo que termine com .exe, .pif e .vbs, pois eles geralmente contêm vírus.

É uma boa ideia instalar um software de antivírus, caso você ainda não tenha um. Há diversas opções de programas eficientes no mercado. Mas não deixe de visitar o site oficial do provedor do software, pois há diversos produtos falsos que alegam proteger o seu computador, mas que na verdade podem infectá-lo com vírus.

Evite fraudes e golpes Online

Fique atento, pois se um negócio ou oferta parecer bom demais para ser verdade, provavelmente é um golpe.

Os criminosos podem contatar você por e-mail, através dos sites que você utiliza, via SMS ou mesmo pelo telefone. Portanto, vale a pena estar bem atento, pois eles conseguem ser bastante convincentes. Veja alguns sinais de alerta:

- Grandes promessas: “Você ganhou na loteria”;
- Grandes ameaças: “A sua conta foi invadida”;
- Um falso sentido de urgência: “Aja agora ou será tarde demais”;
- Sigilo desnecessário: “Não conte a ninguém”;
- ‘‘Oportunidades de Negócio’’ que envolvam manter ou receber dinheiro para estranhos;

Se um anexo parecer suspeito, não o abra. Não instale um software, a menos que venha de um site em que você confie. Caso você ache que há algo errado, verifique

com calma. Se você suspeitar que há algum problema com o seu internet banking pessoal ou empresa, fale conosco primeiro.

Aprenda a identificar emails e sites falsos

Os criminosos utilizam e-mails e sites falsos. Eles usam esses artifícios para enganar as pessoas e tentar obter senhas e dados bancários. O termo técnico para esse tipo de fraude eletrônica é "*phishing*". Por exemplo, eles podem enviar a você um e-mail que parece que foi enviado por nós e que pode conter um link para um site semelhante a este. Quando você tentar fazer o logon, eles podem roubar a sua senha. Eles também podem solicitar que você faça uma ligação ou responda por e-mail. Eles são muito bons em fazer com que seus sites e e-mails pareçam reais, mas os falsos frequentemente possuem algumas características comuns, como:

- Emails ou endereços da web estranhos;
- Desenho mal definido, digitação ou ortografia incorreta;
- Pedem que você faça alguma coisa incomum;
- Um site que exige que você faça login, mas não exibe o símbolo de cadeado na barra de endereço do navegador;

O HSBC jamais pede aos clientes para atualizar ou verificar os seus dados de segurança pessoal por e-mail. Em caso de dúvida, não faça nada. Não clique em nenhum link. Não abra nenhum anexo. Apenas envie o e-mail para **phishing@hsbc.com** e nós investigaremos. Ou então, consulte a página local do seu país para saber como fazer essa denúncia.

Mantenha as suas senhas e informações pessoais seguras

Os fraudadores usam informações pessoais de diferentes fontes para roubar identidades de pessoas. Os vírus são uma forma de fazer isso. Mas eles também usam documentos impressos contendo dados pessoais, como recibos e extratos bancários. Os fraudadores utilizam muitos métodos, como vasculhar lixeiras para obter esses documentos.

Você deve tomar precauções simples para manter os seus dados seguros. Armazene os seus documentos bancários em um lugar seguro e sempre os triture quando não forem mais necessários. Você também pode mudar para extratos e demonstrativos on-line. Enquanto isso, você deve rever os seus extratos bancários e de cartão de crédito para localizar quaisquer operações ou saques incomuns e notificar o banco imediatamente se suspeitar de qualquer discrepância.

Você também deve nos informar quaisquer mudanças em seus dados pessoais (mudança de endereço, por exemplo). Caso você planeje cancelar um cartão de banco/crédito (ou em caso de expiração), destrua imediatamente o cartão, cortando-o em pedaços pequenos para que ele não possa ser reutilizado. Sua senha de internet banking do HSBC, juntamente com as suas outras credenciais de internet banking, permitem acesso às suas contas bancárias.

Não compartilhe informações particulares online

Verifique novamente as configurações de privacidade em redes sociais.

- Qual é o nome de solteira da sua mãe?

- Qual é o nome da primeira escola em que você estudou?
- Qual era a sua matéria favorita na escola?
- Qual é o seu endereço?
- Data de aniversário?
- Número de telefone?

Todas essas informações são úteis para pessoas que queiram roubar a sua identidade ou invadir o seu internet banking pessoal. Você não daria essas informações a um estranho na rua, mas se você utiliza redes sociais, como o Facebook, o Twitter ou o LinkedIn, você pode estar compartilhando dados pessoais em excesso.

É bom ter cautela em relação às informações que você coloca nos seus perfis desses sites. É também uma boa ideia verificar as configurações de privacidade se suas contas de mídia social a fim de se certificar de que você está compartilhando dados pessoais somente com as pessoas em quem você confia.

Lembre-se também de que você deve tomar todas as precauções para manter os seus dados seguros e impedir qualquer uso não autorizado de quaisquer cartões e dados de segurança. Não divulgue os seus dados de segurança a ninguém – vide os termos e condições que se aplicam à(s) sua(s) conta(s) para obter maiores detalhes.

Proteja a sua rede sem fio

Uma rede sem fio permite que você conecte o seu computador à internet sem necessidade da utilização de cabo. Ela geralmente contém um roteador sem fio que utiliza sinais para transferir dados para computadores da rede. Alguns roteadores sem fio são pré-configurados com uma proteção de segurança bem frágil a fim de permitir que os usuários se conectem pela primeira vez – mas isso também implica que outras pessoas também podem acessar com facilidade a sua conta de Internet. Por esse motivo, é sempre aconselhável que você consulte o manual ou o guia on-line para saber como se conectar de forma mais segura por meio de sua rede sem fio – normalmente criando uma senha.

Proteja seus celulares e tablets

Com o aumento do uso de celulares e tablets, eles se tornaram um alvo cada vez mais atraente para os criminosos.

Por exemplo, um criminoso pode enviar a você um e-mail que parece que foi enviado por nós e que pode conter um link para um site semelhante a este. Quando você tentar fazer o logon, eles podem roubar a sua senha. Eles também podem solicitar que você faça uma ligação ou responda por e-mail.

Você pode pensar em:

- Definir e usar um código PIN de segurança. Se você utiliza um celular com recurso de biometria, como um leitor de impressão digital, certifique-se de que a sua é a única impressão digital registrada no aparelho;

- Não armazenar o seu número de telefone e endereço em “casa” na lista de contatos (você não iria querer que um ladrão soubesse o seu endereço e pudesse verificar se você está em casa);

- Ajustar as configurações do telefone de modo que ele trave automaticamente se você não o utilizar por um ou dois minutos;
- Não armazenar senhas e outras informações confidenciais em seu telefone de uma forma que possa ser compreendida por outra pessoa. O seu nome de usuário e senha do HSBC Online Banking não devem ser armazenados em seu celular ou tablet;
- Não use um Apple iPhone com *jailbraker*, um telefone Android com sistema operacional *root* ou qualquer outro dispositivo móvel que tenha sido desbloqueado ou enraizado. Essas são técnicas que removem importantes recursos de segurança que foram incorporados ao seu aparelho pelo fabricante de seu sistema operacional;
- Ao utilizar WiFi, somente use provedores de serviço ou redes de WiFi seguras e confiáveis;
- Desabilite o Bluetooth se você não o estiver usando ou configure o smartphone ou o tablet para o modo não detectável. Isso tornará mais difícil para as pessoas encontrarem o seu dispositivo e enviarem dados maliciosos para ele;
- Cuidado com golpes por meio de correio de voz e mensagem de texto, também conhecidos como "*smishing*". Clicar em links em mensagens de texto pode ser arriscado – tenha cuidado;

Os criminosos também podem criar aplicativos fraudulentos para dispositivos móveis que parecem com os nossos e que podem roubar a sua senha quando você tenta fazer o logon. Certifique-se de que os aplicativos para dispositivos móveis – incluindo teclados virtuais – sejam baixados de app stores confiáveis, tais como Apple App Store e Google Play, e entenda o que você está permitindo que os aplicativos móveis façam antes de instalá-los.

Se você perder o seu telefone, informe imediatamente o seu provedor de telefonia móvel. Anote o número IMEI do seu telefone, pois isso facilitará o trabalho da sua operadora de telefonia para desabilitar o telefone roubado.

Como o HSBC protege você online

Estamos constantemente revendo as formas de proteger os nossos clientes online. A nossa abordagem proativa inclui reuniões com alguns dos maiores especialistas em segurança do mundo para discutir questões-chave e promover iniciativas conjuntas para melhorar a sua segurança online.

Nós protegemos você:

1. Garantindo que as suas transações online são seguras e protegidas. Utilizamos tecnologia e práticas de segurança padrão do setor para proteger a sua conta contra qualquer acesso não autorizado;
2. Usando logons e senhas para ter certeza de que estamos lidando com você. O acesso online à sua conta só é possível após você proceder à autenticação utilizando o ID correto do Internet Banking e dados de segurança;
3. Utilizando autenticação de dois fatores para fornecer uma camada extra de proteção. A chave segura ou dispositivo de segurança é um dispositivo de autenticação de dois fatores que ajudará a protegê-lo contra fraude no Internet

banking. Ele é projetado para garantir que apenas você possa acessar os seus dados pessoais. A autenticação de dois fatores significa que você precisa não somente de uma senha ou PIN, mas também de um dispositivo exclusivo para acessar a sua conta;

4. Criando sessões online seguras. Quando você faz o login no internet banking, aparece um aviso informando que você está em uma sessão segura. Você saberá que está em uma sessão segura se o endereço de URL começar com https:// e um símbolo de cadeado aparecer na parte superior da página como parte da barra de endereço;

5. Utilizando criptografia. Utilizamos criptografia padrão do setor para proteger os seus dados;

6. Utilizando tempo limite de sessão. Se você esquecer de fazer logoff após operar o banco online ou se o seu computador permanecer inativo por um período de tempo durante uma sessão, os nossos sistemas farão o logoff automaticamente;

7. Realizando bloqueios automáticos. Após um número de tentativas incorretas para fazer login, o acesso à sua conta on-line será desabilitado. Para reativar o acesso à sua conta, você deverá ligar para o número do seu serviço usual de suporte ao usuário (helpdesk).