CARTILHA DE SEGURANÇA DA INFORMAÇÃO

BDO

Home-office durante a crise do coronavírus

As últimas semanas foram conturbadas, já que a maioria de nós estávamos nos preparando para enfrentar a realidade da pandemia do Covid-19. Embora toda atenção esteja voltada para como manter os negócios, não podemos tirar os olhos de outra ameaça, uma que pode ter resultados devastadores as Organizações - as violações em nossa segurança da informação.

Com a forte atuação na modalidade de trabalho remoto (home-office), temos observado um salto no número de golpes cibernéticos. O que impõem ainda mais desafios: prover acessos remotos com qualidade e conectividade dos times, além da adoção de medidas de segurança da informação e a proteção dos dados de clientes e funcionários.

Pensando nesses aspectos, a BDO desenvolveu esta lista de recomendações e cuidados que devemos ter constantemente e com reforço adicional, neste momento de isolamento. Confira:

Práticas de proteção de dados que podem ser implementadas

Mude periodicamente a senha

Não use a mesma senha para vários websites e sempre use uma combinação forte, sendo letras maiúsculas e minúsculas, números e outros caracteres. É importante fazer a troca periódica das senhas como forma de proteger tanto as informações pessoais como as da empresa. É importante programar o bloqueio automático da tela após um período sem uso em dispositivos pessoais ou corporativos.

Cuidado com mensagens desconhecidas

Não use o e-mail corporativo para fins pessoais, essa ação auxilia inclusive em potenciais oportunidades de pessoas não autorizadas invadirem o sistema da empresa.

Cuidado com phishing: um e-mail com conteúdo malicioso projetado para enganá-lo; portanto, é importante estar alerta a qualquer fraude e analisar seu conteúdo: remetente desconhecido, arquivos com extensão dupla que

Não compartilhe informações confidenciais

Se você precisar compartilhar informações confidenciais eletronicamente, utilize um ambiente controlado por meio de uma VPN (rede virtual privada) ou de uma rede segura privada, bem como adote criptografia. Nunca divulgue informações confidenciais em uma rede pública não segura. Evite a troca de dados por WhatsApp, SMS, entre outros.

Cuidados com o Wi-Fi público ou doméstico

Wi-Fi gratuitos tem sido grande atrativos as pessoas, porém o risco de exposição de dados é maior, já que a grande maioria não requer autenticação para estabelecer uma conexão de rede, criando uma oportunidade para que pessoas mal-intencionadas obtenham acesso irrestrito à dispositivos não seguros na mesma rede.

Use a autenticação em dois fatores

A autenticação multifatorial (MFA) é definida como um processo de segurança que requer mais de um método de autenticação de fontes independentes para verificar a identidade do usuário. Em outras palavras, uma pessoa que deseja usar o sistema recebe acesso somente após fornecer duas ou mais informações que identifique e valide com maior assertividade.

Utilize a criptografia das informações

Técnicas de criptografia são usadas para proteger os dados e reforçar a confidencialidade e integridade durante a transmissão e o armazenamento. A criptografia também é usada no comércio eletrônico, segurança de rede sem fio e acessos remotos para evitar falsificações. Dados, arquivos, e-mails e até discos rígidos inteiros podem ser criptografados e, com isso, apenas algumas pessoas, de posse da "chave" podem acessar determinadas informações.

O MOMENTO TAMBÉM É DE ATENÇÃO PARA A SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Abril 2020

Mantenha seu computador seguro

- ✓ Execute a verificação completa de varredura de vírus no computador, pelo menos uma vez por semana, muitos softwares de antivírus possuem agenda para pré-agendar a tarefa;
- ✓ Mantenha as definições, e banco de vacinas de vírus atualizados para garantir que seu programa antivírus permaneça eficaz;
- ✓ A instalação de atualizações de software para o seu sistema operacional e programas é fundamental. Sempre instale as atualizações de segurança estável;
- ✓ Evite acessar sites desconhecidos ou fazer download de software de fontes não confiáveis. Esses sites costumam hospedar malware que comprometem de maneira silenciosa seu computador;
- ✓ Ao receber anexos ou links em e-mails inesperados ou suspeitos, não clique!
- ✓ Se precisar se afastar do notebook, celular ou tablet por um período - bloqueie-o para que ninguém mais possa usá-lo;
- ✓ Se você mantiver informações confidenciais em um pen drive ou HD externo, mantenha-os bloqueados.

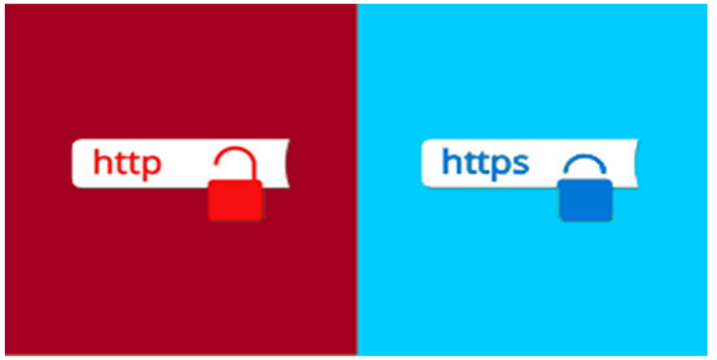
Navegando na internet com segurança

- ✓ Os navegadores costumam ser seu primeiro ponto de contato com a Internet, independentemente do dispositivo que você esteja utilizando, fique atento, atualizações são lançadas frequentemente para garantir que você possa experimentar as últimas novidades da Web;
- ✓ Mesmo que os sites decidam ou imponham o rastreamento de seus dados de navegação, você pode limitar os impactos limpando regularmente o cache do navegador e excluindo cookies indesejados;
- ✓ A navegação privada protege as informações particulares e impede que alguns sites rastreiem seus dados de pesquisa e navegação.

Utilização de Internet Banking

As instituições financeiras (bancos) estão incentivando cada vez mais aos clientes a se tornarem digitais, os riscos associados ao uso de serviços online também aumentam em um ritmo alarmante. Por isso, recomendamos algumas dicas:

- ✓ Nenhuma instituição enviará um e-mail solicitando que você forneça seus detalhes de login. Se você receber um e-mail que parece ser do seu banco solicitando esses detalhes, fique atento, pois pode ser uma tentativa de phishing para induzi-lo a entregar suas credenciais;
- ✓ Verifique se o firewall está ativado e se você está executando um software antivírus. Isso garantirá que você esteja protegido contra cavalos de Troia, keyloggers e outras formas de malware que podem ser usadas para obter acesso aos seus dados financeiros;
- ✓ Sempre encerre sua sessão de banco on-line quando terminar sua atividade. Isso diminuirá as chances de ser vítima de sequestros de sessões e explorações de scripts entre sites;
- ✓ Mesmo se você for o único a acessar o dispositivo, desative o logon automático;
- ✓ Monitore a atividade da conta. Visualize a atividade da conta online regularmente e revise seu extrato periodicamente;
- ✓ Sites seguros têm um endereço da web que inclui um "s" (https em vez de http). Se isso estiver faltando, o site não é seguro.



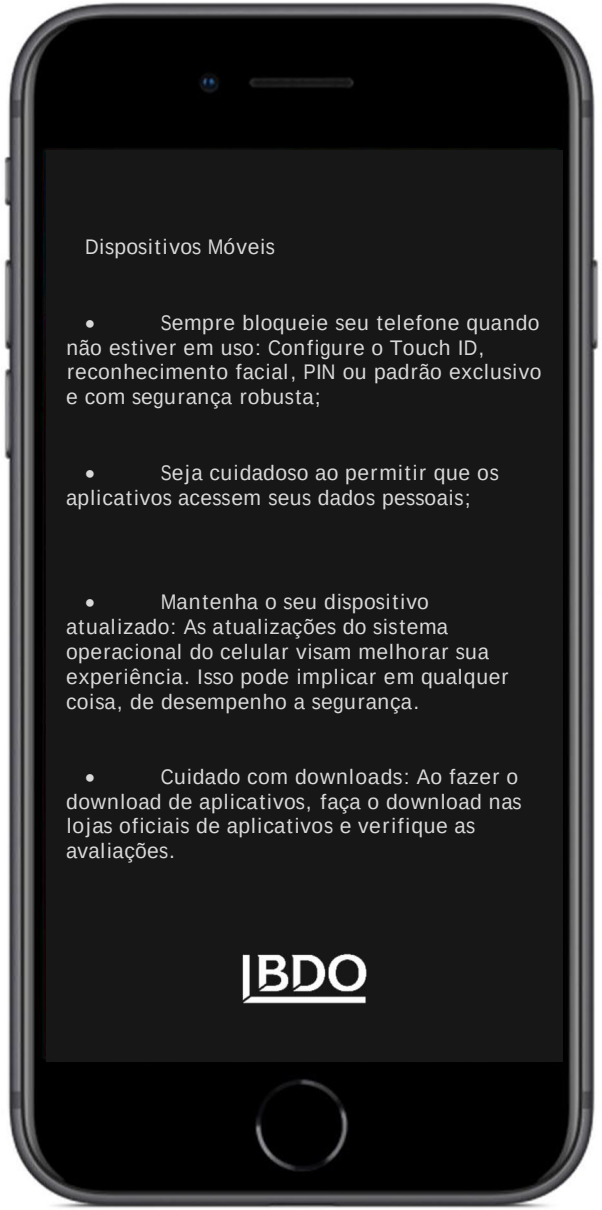
Engenharia Social

O que é: um tipo de manipulação psicológica para levar as pessoas a contornar os procedimentos normais de segurança ou divulgar informações confidenciais.

Como isso pode acontecer:

Em casa: alguém que finge ser do seu banco pode ligar para solicitar sua senha bancária on-line através de um link fornecido por essa pessoa. Sua senha pode ser coletada e usada para esvaziar sua conta.

No local de trabalho: um contratado com o qual sua empresa trabalha pede informações confidenciais que concedem acesso ao seu sistema.



GLOSSÁRIO

Antimalware: um tipo de software projetado para prevenir, detectar e remover software malicioso (malware) em sistemas de TI, bem como em dispositivos de computação individuais.

Cavalo de Tróia (Trojan Horse): um tipo de malware geralmente disfarçado de software legítimo. Os cavalos de Troia podem ser empregados por ciber-ladrões e hackers que tentam obter acesso aos sistemas dos usuários. Os usuários geralmente são enganados por alguma forma de engenharia social para carregar e executar cavalos de Tróia em seus sistemas.

Criptografia: Envolve a criação de códigos escritos ou gerados que permitem que as informações sejam mantidas em segredo. A criptografia converte dados em um formato ilegível para um usuário não autorizado, permitindo que sejam transmitidos sem que entidades não autorizadas decodifiquem de volta em um formato legível, comprometendo assim os dados.

Engenharia Social: termo usado para uma ampla gama de atividades maliciosas realizadas por meio de interações humanas. Consiste na manipulação psicológica para induzir os usuários a cometer erros de segurança ou divulgar informações confidenciais.

Malware: É qualquer programa ou arquivo prejudicial ao usuário do computador. Os tipos de malware podem incluir vírus, worms, cavalos de Tróia e spyware. Esses programas maliciosos podem executar uma variedade de funções diferentes, como roubar, criptografar ou excluir dados confidenciais, alterar ou sequestrar as principais funções de computação e monitorar a atividade do computador dos usuários sem sua permissão.

Phishing: método para tentar coletar informações pessoais usando e-mails e sites fraudulentos.

Spyware: software indesejado que se infiltra no seu dispositivo, roubando dados de uso da Internet e informações confidenciais.

PARA MAIORES INFORMAÇÕES

BDO BRAZIL

+55 11 3848 - 5880

saopaulo@bdo.com.br

www.bdo.com.br