Guia do funcionário seguro

INTRODUÇÃO

A Segurança da informação em uma empresa é responsabilidade do departamento de T.I. (tecnologia da informação) ou da própria área de Segurança da Informação (geralmente, em empresas maiores). Contudo, é dever da empresa como um todo cuidar da informação, já que nas empresas atuais todos os seus integrantes trabalham, de uma forma ou de outra, com dados e informações. Por isso, qualquer um poderia ser responsável por um incidente que afete a segurança dos dados.

Neste contexto, este guia pretende ajudar os funcionários de empresas a cuidarem da segurança da informação na empresa, a partir da compreensão do problema, uma descrição das principais problemáticas, e, finalmente, a enumeração das boas práticas para esse fim.

Um funcionário seguro é aquele que conta com a educação para administrar e utilizar os recursos da empresa de maneira segura e eficiente. Este guia irá ajuda-lo a se tornar um funcionário seguro, ajudando e colaborando com sua organização e com o bem-estar em seu local de trabalho.

A Segurança da Informação é responsável por garantir a integridade, disponibilidade e confidencialidade da informação da empresa, visando cuidar do negócio.

CONFIDENCIALIDADE

A confidencialidade da informação é a necessidade de que ela somente chegue ao conhecimento de pessoas autorizadas

Por exemplo, se um usuário qualquer puder acessar a base de dados de um servidor web, ou qualquer empregado possa conhecer a informação contábil da empresa, a confidencialidade da informação seria violada.

INTEGRIDADE

A integridade da informação é a característica que faz com que seu conteúdo permaneça inalterado, a menos que seja modificado por pessoas autorizadas.

Por exemplo, se um invasor puder modificar os preços de venda de um website, ou um funcionário alheio à área de vendas puder fazê-lo, a integridade da informação seria violada.

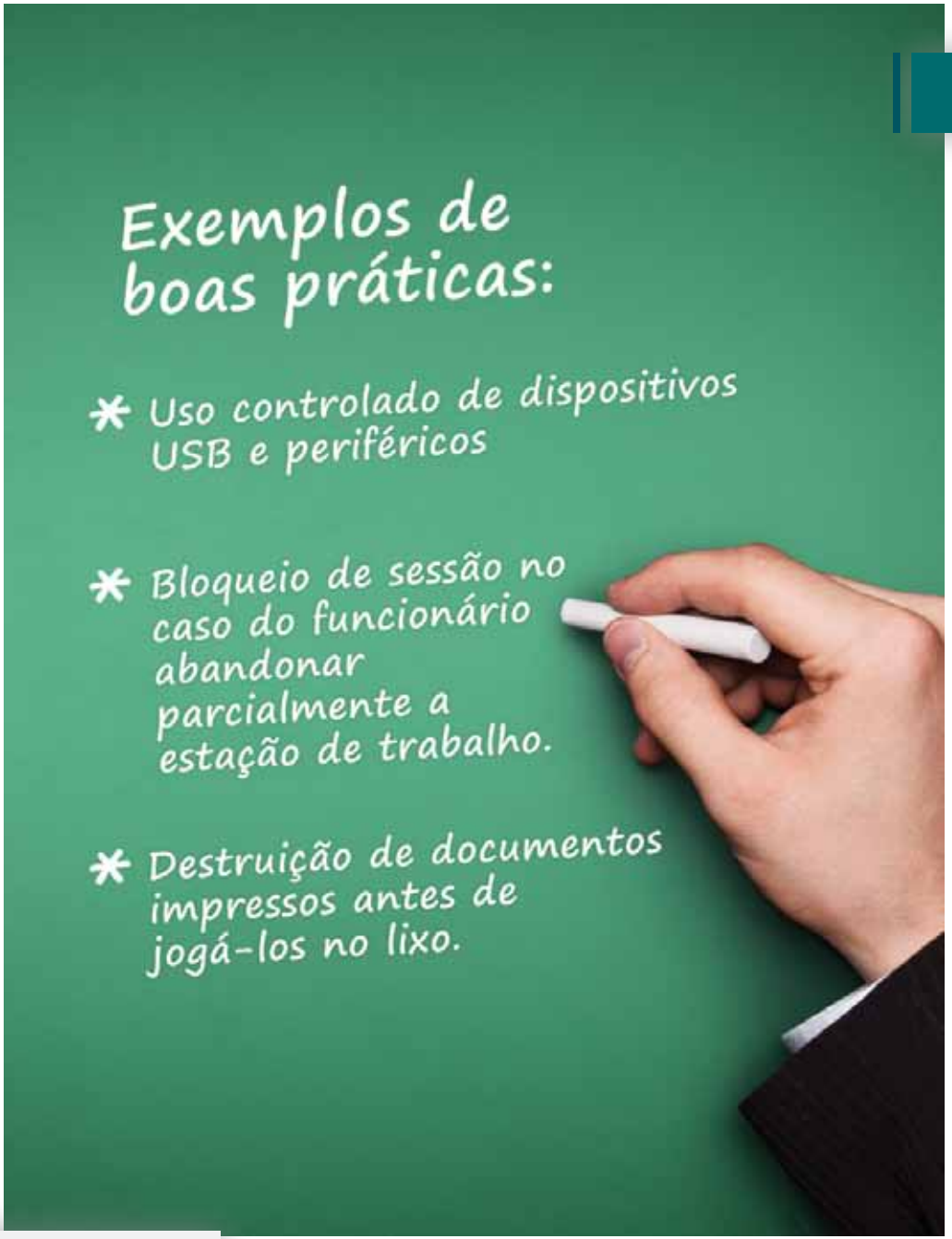
DISPONIBILIDADE

A disponibilidade da informação é sua capacidade de estar sempre disponível no momento em que necessitem dela, para ser processada pelas pessoas autorizadas.

Por exemplo, um ataque contra um sistema de loja online, ou um problema em um servidor que tenha resultado em seu desligamento estariam violando a disponibilidade da informação.

Os incidentes de Segurança da informação podem ser internos ou externos; e maliciosos ou involuntários, como indicam os seguintes exemplos:

	EXTERNO	*INTERNO*
Malicioso	*Um funcionário insatisfeito destrói um documento importante.*	*Um criminoso realiza um ataque de negação de serviço contra o website da organização.*
Involuntário	*Um funcionário perde um dispositivo USB onde havia copiado informação confidencial da empresa.*	*Um excesso de visitas a um site faz com que ele pare de funcionar e perca disponibilidade.*



AS POLÍTICAS DE SEGURANÇA

O ideal é que toda empresa conte com uma política de segurança com o objetivo de que todos os funcionários conheçam a importância da proteção da informação para a empresa. Quando um funcionário entra na empresa, ele deve conhecer os mecanismos básicos para o manuseio seguro da informação e dados.

Em algumas empresas, é feita a entrega de um documento conhecido como políticas de segurança. Quando este documento for firmado, a pessoa confirma que entende e aceita as políticas nele definidas. Desta maneira, se compromete a cumprir as normas de segurança definidas pela organização. É necessário compreender que a existência deste documento

> 1 | *Um **funcionário seguro**, lê, conhece, entende e respeita o que for indicado nas políticas de segurança da empresa.*

No caso de a empresa contar com um documento de políticas de segurança, é necessário consultar o departamento correspondente para saber os procedimentos a seguir e as boas práticas recomendadas pela companhia.

FERRAMENTAS DE SEGURANÇA

As tecnologias são a base da segurança da informação nas empresas.

Geralmente, as tecnologias mais comuns nos computadores dos usuários são as seguintes:

Antivírus

É um software que protege os computadores e suas informações de diferentes ataques de códigos maliciosos. Os antivírus mais eficazes protegem inclusive de forma proativa, contra malware novo ou desconhecido.

Firewall

É um software que pode estar integrado com o antivírus e que protege o computador das conexões de Internet de entrada e saída, utilizadas em diversos tipos de ataques, ou também as tentativas de conexão automáticas que tentam realizar no computador.

Antispam

É um software que muitas vezes está integrado com a solução antivírus ou com o cliente de e-mail e permite à pessoa não receber spam ou e-mails indesejados em sua caixa de entrada corporativa.

> 2 | *Um **funcionário seguro** deve conhecer e respeitar as ferramentas instaladas em seu computador, e estar atento aos seus alertas e avisos.*

Além disso, há muitas outras ferramentas que costumam ser implementadas pelas empresas no perímetro da rede, ou diretamente nos servidores para proteger o negócio e que não são visíveis para os integrantes da empresa, como por exemplo: proxy, IDPS, IPS, firewall perimetral, atualização de pacotes; dentre outras.

MALWARE

O malware (acrônimo de ***mal****icious soft****ware)*** é um dos ataques mais comuns da atualidade. O malware, também conhecido como código malicioso, são arquivos com fins nocivos que, ao infectar um computador, possuem diversas ações nocivas como o roubo de informação, o controle do sistema ou a captura de senhas. Entre muitas das categorias existentes, se destacam os worms, trojans, vírus; dentre outros.

A infecção de um código malicioso pode parecer não impactar em seu trabalho diário, contudo, o que acontece se toda a informação armazenada no computador se perder? Quanto vale o tempo que você ficaria sem poder trabalhar? E quanto à dedicação do departamento de TI para solucionar o problema? Ambas as situações afetam diretamente o rendimento da empresa e, por fim, custa dinheiro.

Além disso, existem códigos maliciosos que são utilizados para o roubo de informação que, inclusive, poderiam afetar diretamente o negócio da empresa ou questões pessoais dos empregados que tiveram ou utilizaram no computador de trabalho.

> **3** | *Um **funcionário seguro** conhece os códigos maliciosos mais comuns e possui boas práticas para evitar a infecção de seu computador.*

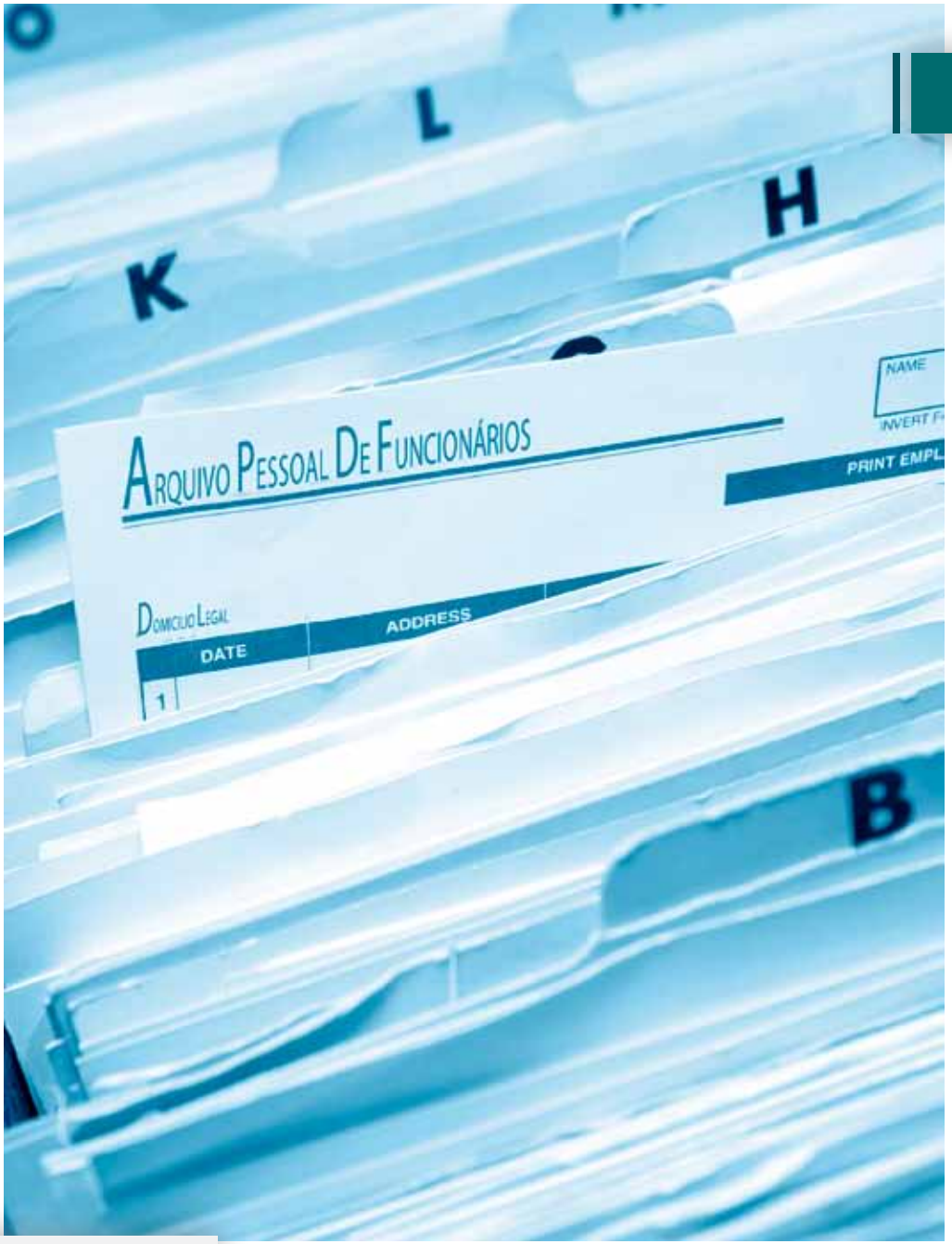
ENGENHARIA SOCIAL

A Engenharia Social é a utilização de habilidades sociais para manipular as ações de uma pessoa. A partir de estratégias de Engenharia Social, os desenvolvedores de códigos maliciosos e criminosos digitais costumam utilizar diferentes meios para enganar, e assim comprometer a segurança da empresa.

Por exemplo, através de e-mails falsos que indiquem a necessidade de oferecer informação confidencial, ou a simulação de aplicações de confiança de sites, falsos chamados telefônicos ou propagação de códigos maliciosos nas redes sociais simulando serem aplicações integradas.

Este tipo de técnica busca conseguir que se realize uma ação que poderia comprometer a Segurança da empresa, afetando também o negócio, como por exemplo, a instalação de um aplicativo ou a inserção de uma senha. Por exemplo, um e-mail falso solicita uma lista de clientes. Se a vítima não se dá conta da veracidade do e-mail, e envia os dados solicitados, poderia entregar informação sensível dos clientes, e assim afetar a confidencialidade da informação. Além disso, há ataques de Internet que utilizam mensagens de engenharia social não diretamente relacionadas à empresa, como pode ser a morte de um famoso ou uma catástrofe natural e que, ao ser vítima deste ataque, que pode resultar na perda de informações sensíveis da empresa.

4 | *Um **funcionário seguro** está atento a esse tipo de mensagens e pode identificar possíveis ataques de Engenharia Social.*



ROUBO DE INFORMAÇÃO

Um dos maiores problemas que podem atingir a organização é o roubo de informação sensível; cuja divulgação pode afetar o negócio. Em alguns casos, este incidente pode ser gerado pelo comportamento inadequado das pessoas e não somente por uma ação maliciosa.

É necessário ter em conta que o roubo de informação não ocorre somente através de meios digitais, já que também envolve o material físico da empresa. Quando, devido a um ataque, descuido ou falta de informação, alguém alheio à empresa acessa os dados confidenciais, seu negócio pode ser afetado de diversas maneiras.

Estatísticas indicam que, em caso de roubo de informação, 62,9% das pessoas deixariam de utilizar o serviço, ou seja, que a empresa poderia perder 6 de cada 10 clientes por não proteger bem seus dados. O impacto que pode significar ser vítima da fuga de informação nos lembra que todos os integrantes da empresa devem cuidar da informação.

> **5** | *Um **funcionário seguro** está atento à informação que é transportada tanto a nível digital como físico, como para evitar a fuga de informação.*

Além disso, quando se desfizer de material impresso com informação confidencial, é necessário destruí-lo de maneira adequada antes de jogá-lo no lixo.

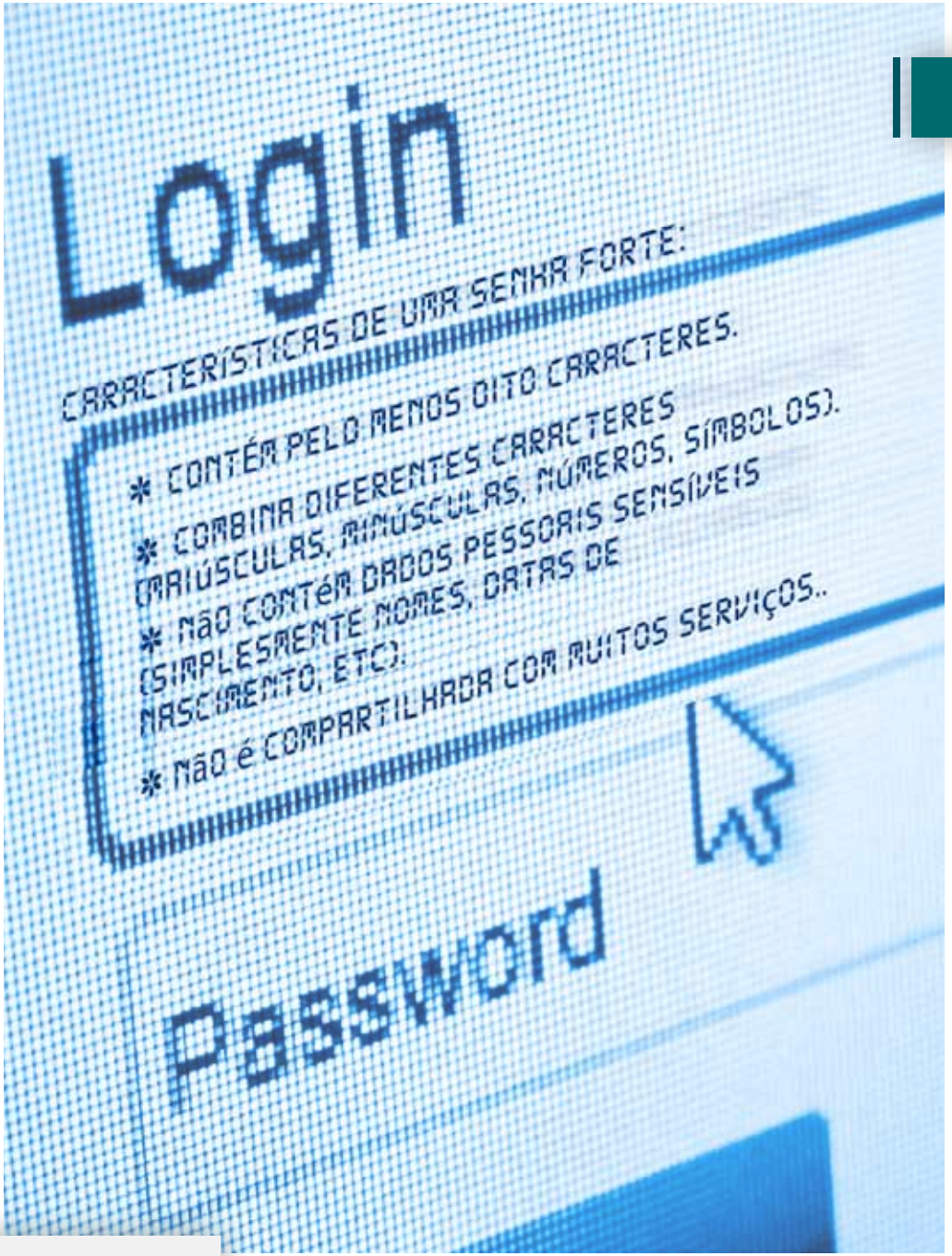
DISPOSITIVOS MÓVEIS

A tecnologia e a incorporação dos smartphones às empresas permitem o acesso à informação em todo momento. A disponibilidade é um dos pilares da segurança da informação. Então, poder ter acesso aos dados quando necessário é algo de grande utilidade, ainda que transportar informações sensíveis em dispositivos móveis poderia ser um grande risco, já que pode abrir as portas à fuga ou ao roubo de informação. Resumindo, o que acontece se o telefone da empresa for perdido ou roubado?

Para evitar ser reativo e ter que sair em busca de uma solução quando surgir o problema, é melhor ser proativo e tentar evitar a ameaça.

Muitas vezes as pessoas que tem um telefone móvel corporativo não levam em conta o cuidado que se deve ter com o dispositivo devido à quantidade de informação confidencial que está disponível nele.

> 6 | *Um **funcionário seguro** utiliza o dispositivo com fins de trabalho, não compartilha o dispositivo com pessoas alheias à organização e o mantém com as melhores práticas de segurança para evitar incidentes sobre a informação armazenada.*



SENHAS

Dada a quantidade de sistemas, plataformas, e-mails e outros serviços da empresa existentes, cada funcionário costuma ter varias senhas. É por isso que uma senha deficiente pode significar o acesso à informação confidencial ou a um sistema por um criminoso virtual ou código malicioso. Tendo isso em conta, é importante que as senhas que são utilizadas na empresa (e também em contas pessoais) sejam fortes: ou seja, que sejam fáceis de decorar e difíceis de decifrar.

Muitas vezes a motivação de criar senhas fortes traz o risco de que sejam esquecidas. Por isso, a utilização de um software para o gerenciamento de senhas é a alternativa mais adequada, não sendo a utilização de cadernos ou papeis pregados no escritório a melhor opção para anotá-las. Além disso, a utilização de senhas diferentes para os mais importantes serviços corporativos também é muito importante.

7 *Um **funcionário seguro** considera a Segurança das credenciais fundamental para seu trabalho, e é por isso que não compartilha com ninguém, utiliza senhas fortes, não as anota em nenhum lugar visível nem utiliza as mesmas senhas para serviços corporativos e pessoais.*

E-MAIL

Há situações em que, para se registrar em algum serviço, ou até mesmo em redes sociais, é exigida uma conta de e-mail para contato. O e-mail corporativo é utilizado como fonte de comunicação da empresa e, na medida do possível, deve evitar sua exposição na Internet.

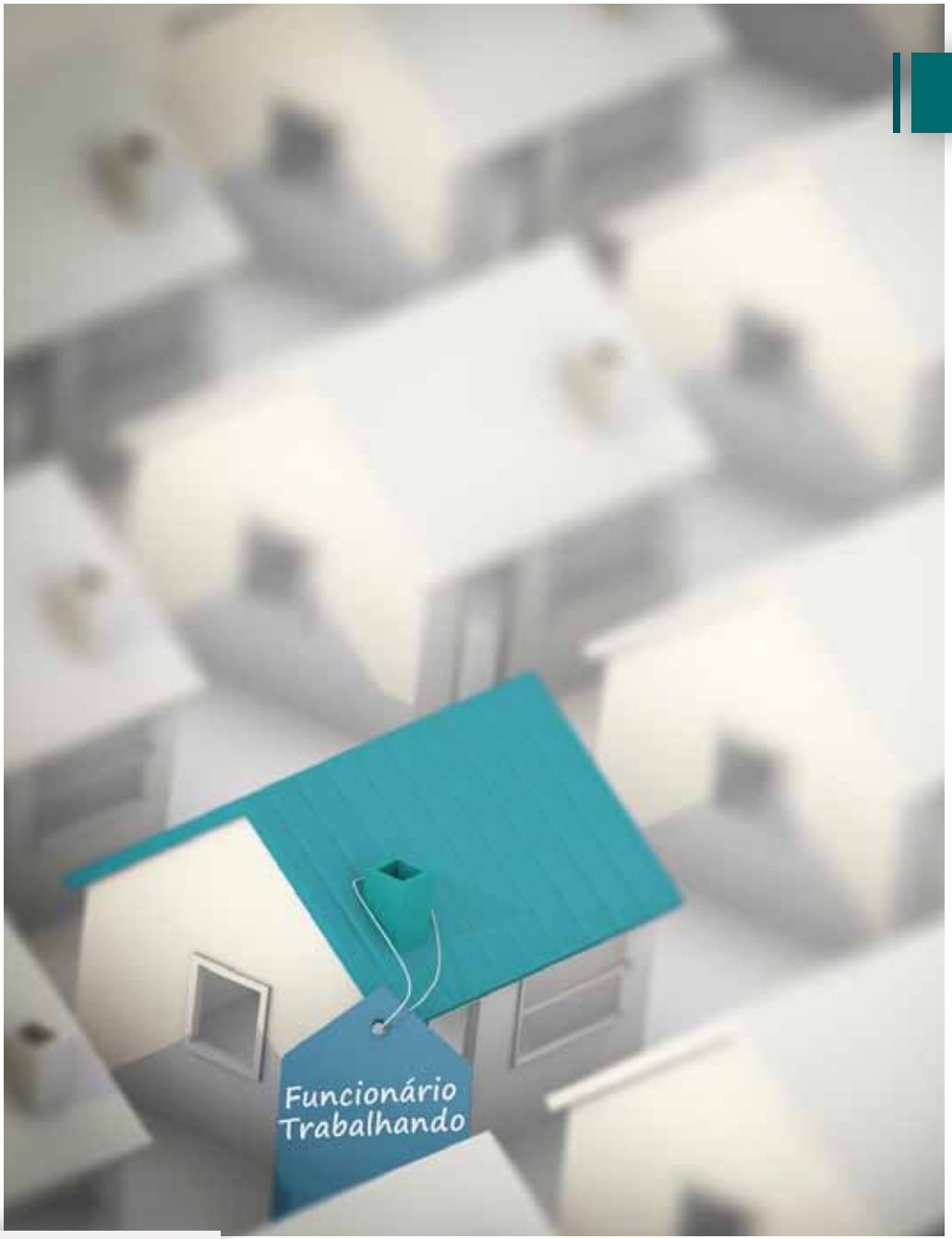
No caso de utilizar o e-mail da empresa para registrar um serviço, pode haver certa exposição desse endereço de e-mail e dessa maneira aumentar a possibilidade de sofrer algum ataque de phishing, assim como também o aumento do número de mensagens não desejadas (spam).

Phishing

O phishing consiste no roubo de informação pessoal e/ou financeira do usuário, através da falsificação de uma instituição de confiança. Desta forma, o usuário acredita inserir os dados em um site de confiança, quando, na verdade, esses dados são enviados diretamente ao criminoso.

Outro aspecto a levar em conta é o comportamento diante de e-mails de origem duvidosa.

> *8* | *Um **funcionário seguro** não acessa links que não provenham de um remetente de confiança já que poderia se tratar de um ataque de phishing ou malware.*



DE CASA PARA O TRABALHO E DO TRABALHO PARA CASA

Atualmente, com a existência dos computadores portáteis, muitos funcionários levam trabalho para casa, e às vezes utilizam ferramentas que não existem no ambiente corporativo, e o computador pode acabar exposto em uma rede que não está devidamente controlada como a da empresa. Ligado a este conceito, é de vital importância tomar certas medidas.

- ***Utilizar um software antivírus no computador pessoal para protegê-lo de possíveis ameaças.***
- ***Manter o sistema operacional sempre atualizado para contar com todos os pacotes de segurança e manter também os aplicativos atualizados.***
- ***Respeitar as políticas de segurança da empresa, mesmo quando estiver fora do ambiente de trabalho.***

Além disso, devemos considerar que há a possibilidade de fuga de informação quando você estiver fora da rede interna da empresa. Desta forma, as medidas apresentadas acima podem ajudar a evitar essa situação.

Como último conselho, quando se leva documentos e papéis importantes para trabalhar fora da empresa, é necessário ter um cuidado especial no que diz respeito ao roubo em lugares públicos, ou até mesmo na sua residência. Além disso, esses documentos devem ser manipulados tendo em conta o nível de confidencialidade que exigem.

No caso da utilização de dispositivos de armazenamento USB ou memórias, sempre é necessário realizar uma análise com um antivírus no momento de inseri-los no computador (seja no ambiente corporativo, como no pessoal). Para evitar infecções dos dispositivos de armazenamento a partir do seu uso no equipamento doméstico, sempre é recomendável contar com uma solução antivírus nesse âmbito.

9 | *Um **funcionário seguro** cuida da informação da empresa, inclusive fora do âmbito corporativo.*

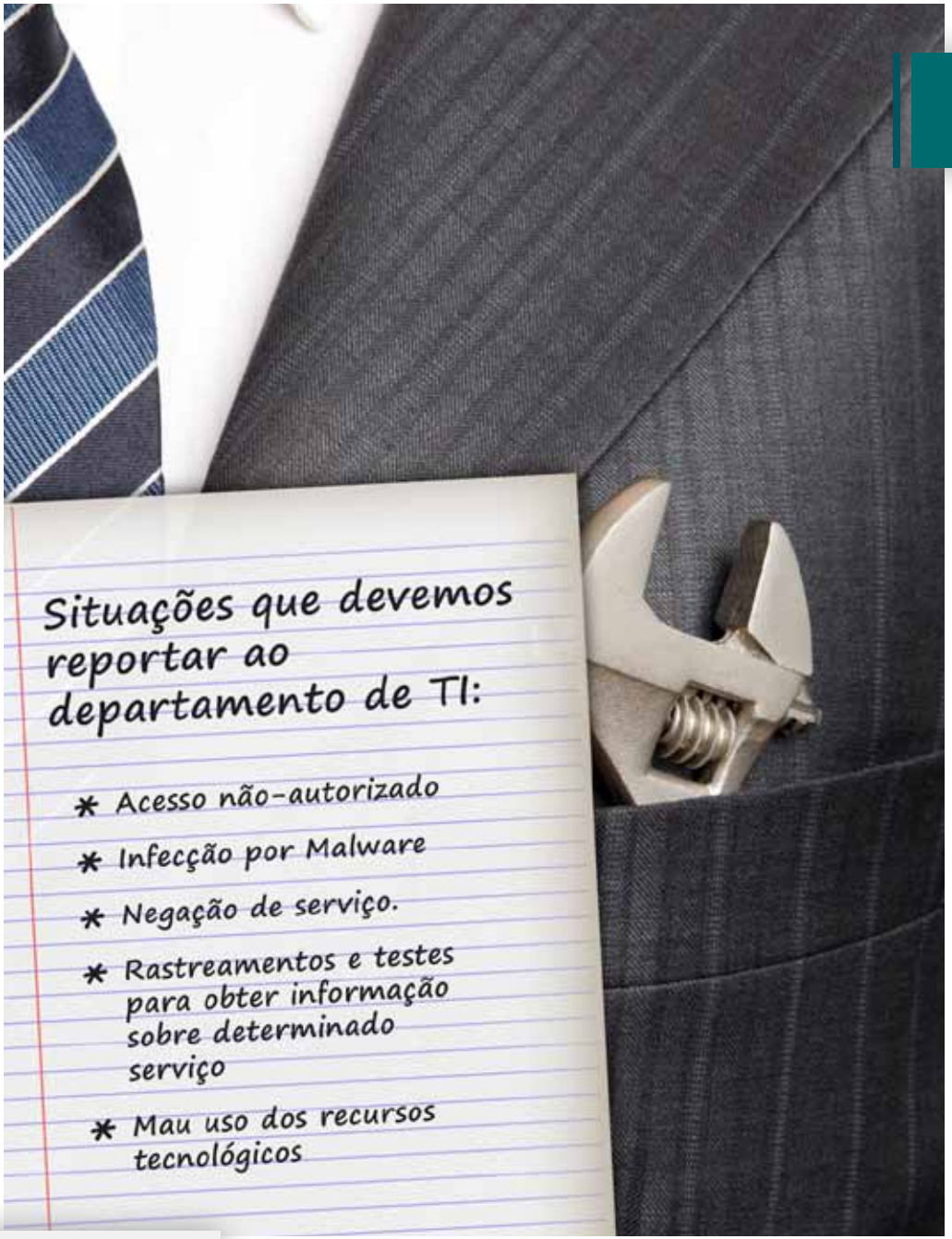
COMPUTADORES DO TRABALHO EM REDES WIFI PÚBLICAS

É comum utilizar o computador portátil do trabalho para se conectar a redes WiFi públicas, como por exemplo, redes de bares, cafés, aeroportos, etc. Nesses casos, devemos considerar que a segurança estará ligada aos controles existentes na rede. Em muitos casos, esses controles são inexistentes, assim como a ausência de senha para realizar a conexão WiFi.

É por isso que se recomenda ao usuário realizar conexões sensíveis, como por exemplo, acessar o e-mail corporativo, já que a rede pode estar exposta e a informação sem nenhum tipo de criptografia. Com isso, muitos dos dados podem ser visíveis para outra pessoa que esteja conectada à mesma rede.

No caso de se utilizar um computador público para acessar, não devemos acessar arquivos com informação confidencial de forma local, já que esses arquivos podem ficar acessíveis no computador e serem vistos por qualquer pessoa que utilize o mesmo computador no futuro.

10 | *Um **funcionário seguro** utiliza uma conexão privada virtual (VPN) quando se conecta a redes sem fio públicas.*



QUANDO CHAMAR O DEPARTAMENTO DE TI PARA UM INCIDENTE DE SEGURANÇA?

Há casos em que se pode suspeitar que o sistema ou inclusive a empresa completa tenham sido comprometidos. No caso de suspeitar que realmente tenha ocorrido um incidente, deve-se avisar o departamento de TI ou segurança imediatamente, já que são encarregados de controlar esse tipo de situação.

No caso da ocorrência de algum incidente de Segurança de qualquer tipo, devemos comunicá-lo imediatamente ao departamento correspondente.

> 11 *Um **funcionário seguro** informa imediatamente antes de qualquer suspeita um incidente de Segurança. É preferível uma denúncia equivocada, que não resulte em ameaça, que a existência de uma ameaça que nunca tenha sido reportada.*

BOAS PRÁTICAS DE UM FUNCIONÁRIO SEGURO

1

POLÍTICAS DE SEGURANÇA
Ler e respeitar as políticas de Segurança da empresa..

2

BLOQUEIO DE SEÇÃO
Bloquear a sessão quando o posto de trabalho for abandonado.

3

DESTRUIR DOCUMENTOS
Destruir documentos impressos sensíveis antes de jogá-los fora.

4

ACESSO A SITES DE REPUTAÇÃO DUVIDOSA
Evitar o acesso a sites de reputação duvidosa.

5

DOWNLOAD DE APLICATIVOS DESCONHECIDOS
Evitar o download de aplicativos não conhecidos que poderiam ser malware.

6

ACESSO A SITES DUVIDOSOS
Evitar a inserção de informação em sites duvidosos que poderiam ser phishing.

7

INFORMAÇÕES PESSOAIS
Evitar compartilhar informação com pessoas não autorizadas a acessá-las.

8

DISPOSITIVOS CORPORATIVOS
Utilizar o dispositivo móvel corporativo somente com fins de trabalho, e não compartilhá-lo com pessoas alheias à empresa.

9

SENHAS FORTES
Utilizar senhas fortes.

10

SENHAS PESSOAIS
Não compartilhar senhas pessoais ou de trabalho.

11

TECNOLOGIAS DE SEGURANÇA
Conectar-se somente às redes WiFi conhecidas ou utilizar tecnologias de segurança como VPN, no caso de acessar a redes sem fio públicas.

12

REPORTAR INCIDENTES DE SEGURANÇA
Reportar qualquer suspeita de incidente de segurança para a organização.

BOAS PRÁTICAS DE UM FUNCIONÁRIO SEGURO - EM CASA

Na sua casa, também é recomendado ter cuidado com seu sistema. Cuidar de suas informações pessoais é uma boa maneira de cuidar também das informações da empresa. Para isso, recomendamos as seguintes práticas de segurança:

1. ***LINKS SUSPEITOS***
   Evitar links suspeitos.

2. ***ACESSO A SITES DE REPUTAÇÃO DUVIDOSA***
   Não acessar sites de reputação duvidosa.

3. ***ATUALIZAÇÃO DO SISTEMA OPERACIONAL***
   Atualizar o sistema operacional e os aplicativos.

4. ***APLICATIVOS OFICIAIS***
   Baixar aplicativos de sites oficiais.

5. ***TECNOLOGIAS DE SEGURANÇA***
   Utilizar tecnologias de segurança.

6. ***INFORMAÇÕES EM FORMULÁRIOS DUDOSOS***
   Evitar a inserção de informação pessoal em formulários duvidosos.

7. ***RESULTADOS DE BUSCADORES***
   Ter precaução com os resultados trazidos por sites de busca.

8. ***CONTATOS CONHECIDOS***
   Aceitar somente contatos conhecidos.

9. ***ARQUIVOS SUSPEITOS***
   Evitar a execução de arquivos suspeitos

10. ***SENHAS FORTES***
    Utilizar senhas fortes.

CONCLUSÃO

Sendo parte de uma empresa - não importa a tarefa que você desenvolve ou a área em que atua - proteger informações confidenciais da organização é também proteger o negócio. Devido a isso, tanto a utilização das tecnologias para segurança, como a educação de seus usuários sobre as ameaças e técnicas de proteção, ajudam a garantir a continuidade do negócio.

Qualquer interrupção ou complicação ocasionada pela infecção de um código malicioso ou ataque a sua organização impacta diretamente em sua imagem, na empresa e na confiança que os clientes podem ter da companhia. Entender a segurança corporativa e manter-se informado é algo valioso para sua empresa.

Fan Page
http://www.facebook.com/esetsoftware

Siga
@eset