FORMAÇÃO DE SEGURANÇA DA INFORMAÇÃO

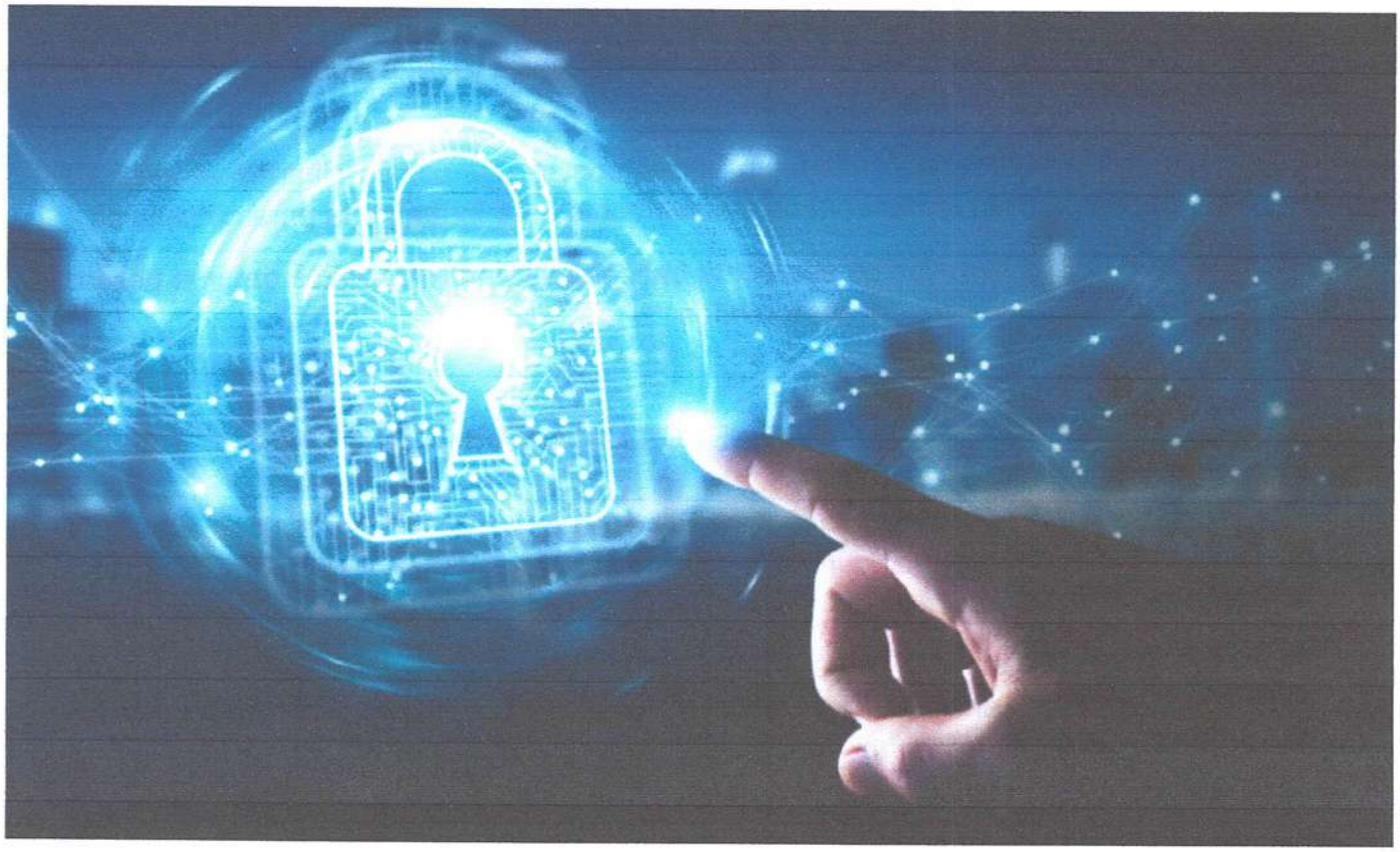
PREVCAR

Profº Ms Fabiano Aparecido de Oliveira

REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE CARIRIAÇU-CE

PREVCAR

Segurança na internet



Nós estamos sendo vigiados na internet constantemente.

Sites de bancos, redes sociais e até plataformas de buscas armazenam os nossos dados diariamente para melhorar a "oferta" de navegação.

No entanto, é preciso ter cuidado. Tantos olhos assim em nossos dados, o tempo todo, pode nos deixar vulneráveis a invasores inesperados.

Os hackers podem estar em qualquer lugar: desde aquele site de compras com o sapato maravilhoso, até a plataforma de assinatura do seu jogo favorito.

Eles ficam lá, apenas esperando você inserir todos os seus dados para coletá-los.

E não é só isso...

Quem não se lembra do vazamento de dados da Netshoes? Ao todo, 2,5 milhões de dados pessoais de clientes vazaram na internet entre 2017 e 2018. Mais de R$ 500 milhões em indenizações e muitos transtornos para cancelar cartões de crédito ou explicar uso indevido de nomes e documentos.

E para quem pensa que apenas sites de compras sofrem com hackers, basta lembrar de dois vazamentos de dados do Banco Inter, que deixou mais de 2 milhões de clientes completamente expostos!

Até mesmo o Banco do Brasil sofreu com ataques dos hackers no seu antigo aplicativo, que precisou ser descontinuado.

Por isso, saber como navegar na internet com segurança é essencial para não ter preocupações com dados circulando livremente na internet.

Além disso, informações publicadas em redes sociais ou compartilhadas através de aplicativos de mensagem, também podem servir como uma forma porta para criminosos.

Para evitar que toda a sua vida ou sua conta bancária vá parar nas mãos de uma pessoa estranha, alguns cuidados devem ser tomados.

QUAIS OS RISCOS DE SEGURANÇA NA INTERNET?

Esteja você fazendo transações bancárias on-line, se conectando com amigos, enviando e-mails ou consultando o mercado imobiliário em sua área, a Internet se tornou uma parte essencial da vida cotidiana.

O que você talvez não saiba é que esse recurso incrível também é um terreno fértil para atividades criminosas - onde todos os seus movimentos podem ser monitorados e suas informações comprometidas.

Mas se você reservar um tempo para aprender sobre as ameaças e riscos comuns, a segurança online e a proteção de si mesmo podem ser fáceis.

Atividades Online

A Internet é uma parte importante da vida cotidiana. Descubra o que você precisa saber para se manter protegido.

- E-mail
- Banco e finanças
- Rede social
- Móvel
- Comprar online
- Jogos e Entretenimento Online
- Download e compartilhamento de arquivos
- Protocolo de voz sobre Internet (VoIP)

Ameaças comuns

Phishing. Pharming. Falsificação. Não sabe o que isso significa? Esse é um bom lugar para começar.

- Botnets
- Negação de serviço distribuída (DDoS)
- Hacking
- Malware
- Pharming
- Phishing
- Ransomware
- Spam
- Spoofing
- Spyware
- Cavalos de Tróia
- Vírus
- Escutas Wi-Fi
- Worms

Golpes e Fraudes
Conheça os diferentes tipos de fraudes e fraudes para que você possa reconhecê-los.

- Golpes por e-mail
- Golpes de phishing e smishing
- Golpes em concursos e sorteios
- Golpes de namoro online
- Golpes de redes sociais
- Diretório Scam
- Chamadas fraudulentas

São muitas as possibilidades de ser hackeado ou de ter seus dados vazados. Por isso, é sempre bom ficar atento aos oito pontos principais de segurança na internet. Confira:

São muitas as possibilidades de ser hackeado ou de ter seus dados vazados.

DICAS PARA GARANTIR A SEGURANÇA NA INTERNET

1. Fique atento para sites desconhecidos
Desconfie de sites com endereços desconhecidos, com erros de design e grafia ou com ofertas muito tentadoras.

Alguns golpes são aplicados a partir de sites que oferecem produtos abaixo do mercado, mas que não contam com imagens de boa qualidade, erros gramaticais ou falta de informação.

Além disso, a maioria desses sites não oferecem um endereço seguro (https) ou garantia de proteção ao cliente (Norton Security e etc).

2. Evite instalar softwares suspeitos

Sabe quando um site manda você instalar um software antes de baixar um filme ou música? Ou até aquela barra de ferramentas que promete organizar a sua vida e o seu computador? Desconfie.

Diversos softwares são responsáveis por vigiar os seus passos no computador, reconhecer e gravar suas senhas e dados e também controlar a sua webcam.

3. Altere as suas senhas regularmente

Isso é sempre muito difícil para o usuário: gerenciar senhas exclusivas para diferentes contas. Mas é fundamental criar senhas cada vez mais fortes para impedir ataques de força bruta, por exemplo.

Se um invasor tiver acesso à sua conta pessoal, poderá promover ações maliciosas "em nome" do titular da conta, o que pode levar a inconvenientes legais; ou até mesmo usar dados pessoais para promover outros golpes e gerar perdas financeiras.

4. Mantenha o seu firewall ativado

Um firewall é um aplicativo que protege seu computador contra hackers que obtêm acesso não autorizado ao seu computador.

A configuração de um firewall pessoal reduzirá drasticamente a possibilidade de o seu computador ser atacado por ameaças da Internet.

5. Evitar clicar ou baixar os anexos de e-mails desconhecidos

Cuidado ao abrir e-mails de pessoas ou fontes desconhecidas, especialmente quando eles não são solicitados.

Clicar em links ou fazer download de anexos pode infectar seu computador com vírus ou sujeitar você a fraude, malware ou fraude. Alguns vírus danificam seu computador, enquanto outros têm a capacidade de roubar suas informações pessoais e, finalmente, sua identidade. Seja cético ao receber e-mails que pareçam vir do seu banco ou de outra

instituição financeira, especialmente se solicitarem que você verifique ou insira informações pessoais ou financeiras.

Cuidado com os golpes que usam links em e-mails direcionando você para um site ou fornecendo um número de telefone para ligar. Alguns links em e-mails podem enganar. Considere digitar seu próprio link para os bancos e empresas ou procure o número de telefone.

Em geral, cuidado com golpes de e-mail e sites que tentam induzi-lo a compartilhar suas informações pessoais.

Um site que pareça legítimo pode ser configurado rapidamente. Lembre-se de que representantes de atendimento ao cliente legítimos nunca solicitarão informações ou senhas pessoais.

Considere não responder a e-mails não solicitados, nunca clique nos links desses e-mails e seja cauteloso se você for solicitado a responder rapidamente.

6. Mantenha o seu antivírus atualizado

Atualmente, o software de segurança é essencial, independentemente do uso do seu computador. No mínimo, 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.

Você também deseja manter o sistema operacional e outros softwares atualizados para garantir que não haja falhas de segurança.

7. Verifique o certificado de segurança do site

Você entra em uma casa que não conhece e deixa todos os seus documentos em cima da mesa? O mesmo vale para o ambiente virtual. Ao se deparar com sites desconhecidos, verifique sempre o certificado de segurança e as informações de privacidade.Caso não tenha nada disso, é melhor evitar.

Caso seja algum site de compras ou rede social indicada por algum amigo, verifique todos os parâmetros de segurança. Antes de inserir seus detalhes de pagamento em qualquer site, verifique se o URL começa com https - o "s" significa "seguro".

Se um site apresentar erros tipográficos ou gramaticais óbvios ou nenhuma evidência de informações de segurança ou símbolos reconhecidos, evite-o.

8. Tenha cuidado ao repassar informações pessoais pela internet

Pense antes de publicar qualquer coisa online ou compartilhar informações em e-mails. O que você publica online pode ser visto por qualquer pessoa.

Compartilhar informações pessoais com outras pessoas que você não conhece pessoalmente é um dos seus maiores riscos online.

Considere remover seu nome de sites que compartilham suas informações pessoais obtidas de registros públicos (incluindo seu número de telefone, endereço, avatares de mídia social e fotos) com qualquer pessoa na Internet.

As fotos tiradas de smartphones incorporam as coordenadas GPS na foto, o que permitirá que outras pessoas saibam a localização de onde a foto foi tirada e pode ser usado para encontrá-lo.

Cuidado ao postar fotos em sites de mídia social online. Lembre-se de que as fotos publicadas on-line podem ser copiadas, alteradas e compartilhadas com muitas pessoas sem o seu conhecimento ou consentimento, a menos que você use as configurações de privacidade para limitar quem tem acesso às fotos.

Tenha cuidado ao repassar informações pessoais pela internet

9. Aprenda sobre o mundo virtual

Informe-se. Não há nada melhor do que saber maneira de se prevenir das ameaças on-line. Procure sempre informações na internet, cursos, palestras e maneiras de se proteger. E caso haja algum problema com seu computador, leve seu equipamento até um **especialista em T.I** pois esses profissionais são os mais indicados para resolver qualquer problema operacional ou de contaminação que seus aparelhos venham a ter.

10. Não salve suas senhas

Elas são restritas e de uso pessoal. Por isso, não salve suas senhas no computador - nem no seu e muito menos em algum de uso compartilhado. O mundo da internet é muito perigoso e um deslize pode fazer você ter seus dados descobertos. Melhor prevenir que remediar.

11. Cuidados com os links que você clica

Atenção redobrada nesse caso. Muito cuidado com os links que você clica, principalmente nas redes sociais como Facebook e Twitter. Histórias diferentes, curiosas e engraçadas demais podem ser uma armadilha para sua proteção contra vírus e ataques cibernéticos. Use do bom senso e pesquise sobre o assunto, com o intuito de arranjar uma fonte confiável para o tema.

12. Não acredite em super promoções da internet

A famosa expressão norte-americana "não existe almoço grátis" é verdadeira no mundo capitalista em que vivemos. Propagandas de objetos com descontos astronômicos, em sites que você nunca ouviu falar, e anúncios de que você foi o milionésimo a acessar alguma página na internet são indícios de que há algo errado. Um vírus pode invadir seu computador, caso clique em links encontrados em situações parecidas, e ter acesso aos seus dados pessoais.

13. Fique atento aos falsos e-mails e anexos

Muitas vezes os e-mails são corrompidos e falsos e-mails caem na sua caixa de entrada. É muito comum se tratarem de assuntos como traição, emprego, dinheiro e rastreamento de encomendas. Não clique em links ou anexos enviados por endereços virtuais desconhecidos.

DICAS FUNDAMENTAIS PARA TER MAIS SEGURANÇA AO ACESSAR A INTERNET NO TRABALHO

Não nos vemos mais sem o uso da internet, ela sem dúvida nos trouxe praticidade a um milhão de facilidades no dia à dia e nosso teste de velocidade mostra que as velocidades de conexão estão cada vez maiores.
Mas se já devemos ter certos cuidados com seu uso em casa, no trabalho a atenção deve ser redobrada. Qualquer descuido por mais que não seja proposital, pode causar danos a sua imagem e da empresa, pois por diversas vezes conteúdos indesejáveis.
Se você quer proteger seu trabalho e sua imagem profissional, confira algumas dicas de que não se deve fazer no ambiente online.

Imagem da empresa e e-mail do trabalho

O índice de empresas que utilizam mídias sociais em seu ambiente de trabalho cresce a cada dia, mas o uso deste tipo de mídia é controlado.
Sendo assim evite posts que possam ter conflito com a empresa onde trabalha, tenha em mente que milhares de pessoas terão acesso as informações publicadas e dependendo do conteúdo pode causar danos a imagem da empresa.
Não utilize o e-mail de trabalho para outros fins, o e-mail que você utiliza no trabalho deve ser destinado apenas para assuntos do trabalho.

Vocabulário

Cuidado com o vocabulário! Nunca use palavrões e evite as gírias.

Assuntos internos

Deve-se tomar cuidado com a divulgação de informações internas da empresa. Às vezes uma simples informação, pode ser valiosa para a concorrência.

Não repassar senhas

Caso possua senhas personalizadas para acessar os serviços de internet da empresa, não as compartilhe com ninguém.
Essas informações podem ser repassadas facilmente, e lembre-se, se algo acontecer, automaticamente a responsabilidade estará em suas mãos.
Sendo assim sempre tome muito cuidado, afinal você pode colocar seu emprego em risco.

Respeite o uso de banda larga da internet

Muitas empresas proíbem o uso da internet ou de sites específicos no ambiente de trabalho por existir abuso de certos funcionários.
Mas se sua empresa libera o uso da mesma, não abuse! Respeite os limites e use apenas para fins do trabalho e não use mais do que você tem direito. Mesmo que não exista uma proibição, o exagero pode prejudicar.
Se você quer acessar suas redes sociais, baixar arquivos ou assistir vídeos em streaming, deixe para utilizar em casa, mas caso precise verificar algo no trabalho verifique se não está deixando a velocidade de internet reduzida deixando os demais computadores lentos.

CUIDADOS NO USO DA INTERNET COMO INSTRUMENTO DE TRABALHO

Todo trabalhador, seja ele público ou privado, deve observar cuidados básicos no usa da internet no ambiente de trabalho.

O uso adequado da internet nos ambientes de trabalho deveria ser hoje o principal assunto tratado nos treinamentos iniciais de todo funcionário recém admitido, já que se trata de um dos ferramentais mais importantes dentro de uma empresa. É certo que há muitas profissões em que as atividades são feitas sem o uso de computadores, mas todos, até mesmo o trabalhador braçal, podem usufruir dos benefícios da internet, por exemplo, fazendo algum curso de aprimoramento por meio do estudo à distância, ou ampliando sua rede de relacionamentos via redes sociais. O fato é que o moderno universo on line precisa ser corretamente explorado por todos, seja qual for sua profissão. Suas regras básicas precisam ser bem compreendidas e seus recursos devem ser usados de forma ética, sobretudo quando se trata da utilização da internet nos locais de trabalho. Quem se coloca alheio a essa realidade, seja patrão ou funcionário, pode sofrer algumas conseqüências indesejáveis, além de deixar de aproveitar os benefícios que podem ser colhidos do universo on line.

No âmbito público também já se reconhece a importância de explorar os benefícios das redes sociais. A Portaria Nº 38, de 11 de junho de 2012, que homologa a Norma Complementar nº 15/IN 01/DSIC/GSIPR, a qual estabelece as Diretrizes para o uso seguro das redes sociais na Administração Pública Federal (APF), prevê, no seu item 2.1 que: "O fenômeno das redes sociais é uma realidade mundial. No Brasil, o seu uso vem crescendo exponencialmente, inclusive nos órgãos e entidades da APF, como uma ferramenta para aproximarem-se ainda mais do cidadão brasileiro e prestar atendimento e serviços públicos de forma mais ágil e transparente, em consonância com os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência.

O governo federal, por meio de sua política de Governo Eletrônico, assume a responsabilidade de investir da maneira correta na interação com os cidadãos por meio da internet e seus recursos. Já se estabeleceu em todas as esferas governamentais e em quase todo o país a regra segundo a qual "os administradores dos perfis nas redes sociais devem buscar sugestões para as políticas do governo, utilizar estratégias para estimular a interação com os usuários, disseminar boas práticas e promover respostas ágeis aos questionamentos feitos pelos usuários."[3]

O Decreto nº 7.675, de 20 de janeiro de 2012, no seu art. 35, inciso IV, prevê que compete ao Departamento de Governo Eletrônico "definir e publicar padrões e melhores práticas de uso da internet, inclusive de redes sociais, para melhoria da gestão e disponibilização de conteúdos públicos digitais".

O aumento dos investimentos em internet e redes sociais tem sido encarado como um ponto fundamental tanto para quem trabalha no comércio como para a implementação de políticas públicas e aprimoramento do atendimento aos cidadãos.

Recentemente foi publicada a Lei n. 12.695, de 23 de abril de 2014, que trata dos princípios, garantias e deveres para o uso da Internet no Brasil. Ela prevê explicitamente, em seu art. 4º, que a internet no Brasil tem por objetivo a promoção do direito de acesso à internet a todos e do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos.

No ambiente virtual, contudo, as pessoas e instituições precisam conhecer melhor as regras éticas de relacionamento na rede. Alguns casos servem de exemplo para termos uma noção correta da importância de se ter cuidado quanto ao uso da internet nos ambientes de trabalho, eis alguns que tomaram destaque:

Em decisão unânime prolatada em novembro de 2012, no Recurso de Revista de n.º 625-74.2011.5.09.0001, o Tribunal Superior do Trabalho manteve entendimento do Juízo da 1ª Vara de Trabalho de Curitiba, em que uma ex-empregada da Clínica Veterinária Portal dos Bichos foi condenada a indenizar seus dois patrões no valor de R$ 2.000,00 cada, por danos morais. O motivo da condenação foi o fato de a ex-empregada, após a demissão, ter difamado os requerentes pelo site de relacionamentos Orkut, fazendo comentários depreciativos, além de ter confessado que maltratava os cachorros de propriedade dos requerentes. O Ministro relator entendeu que "as ofensas e expressões pejorativas proferidas pela reclamada, constantes das atas notariais juntadas aos autos, causaram dano de ordem moral aos reclamantes, pois lhes atingiram a dignidade, a intimidade e a honra, causando constrangimento e angústia."

Em outro processo, a Segunda Turma do TST negou o Agravo de Instrumento em Recurso de Revista de n.º 5078-36.2010.5.06.0000 de uma enfermeira da Unidade de Tratamento Intensivo (UTI) do Prontolinda Ltda., em Olinda (PE), que foi demitida por justa causa após postar, numa rede social da internet, fotos da equipe de trabalho tiradas durante o expediente. Na decisão mantida ao final da ação ficou reconhecido que a conduta da enfermeira foi grave e justificou sua demissão. Os juízes entenderam que o empregador agiu corretamente ao aplicar a justa causa, porque as fotos revelam que a equipe estava em "ambiente de brincadeiras nitidamente inadequadas". O acórdão cita inclusive episódio com "uma das enfermeiras semiagachada e uma mão supostamente tentando apalpá-la"[4]

No processo número AIRR-1542/2005-055-02-40.4, a sétima turma do TST aceitou a tese de que não há ilicitude no ato da empresa que acessa caixa de correio eletrônico corporativo de empregado, se o empregado estava utilizando o e-mail para assuntos particulares. Nesse caso, segundo o Tribunal, o acesso das mensagens pelo empregador não representa violação de correspondência pessoal nem de privacidade ou intimidade, já que o computador, a internet e o e-mail corporativo são ferramentas fornecidos pela empresa para utilização exclusiva para o trabalho.[5]

Como já foi comentado, é preciso entender que o ambiente da internet tem regras semelhantes às do ambiente físico. A ética necessária para se portar em um território virtual são basicamente as mesmas usadas no mundo real. Fazendo esse alerta aos internautas, a escritora Patrícia Peck Pinheiro, especialista em Direito Digital, cita em sua obra[6] Direito Digital algumas dicas interessantes para as empresas e organizações

públicas realizarem um monitoramento corporativo eficiente das atividades on line de seus funcionários:

- Evitar subjetividade e/ou generalizações;
- Deixar claro o conceito de identidade digital (não apenas de senhas) e alinhar com alçadas e poderes;
- Deixar claro que há monitoramento (e prever as duas hipóteses tanto para fins de segurança como de produtividade);
- Deixar claro que há inspeção física de equipamentos da empresa, particulares e/ou de terceiros;
- Deixar claro que os recursos devem ser usados só para fins profissionais;
- Prever que a mera tentativa de burlar também é uma infração às normas;
- Deixar clara a proibição de infração de direitos autorais, prática de pirataria, pornografia, pedofilia, guarda, manuseio de conteúdos ilícitos ou de origem duvidosa e que a empresa vai colaborar com as autoridades;
- Tratar sobre a má conduta (infração mais ética do que jurídica);
- Prever a divulgação da norma;
- Deixar claro papéis e responsabilidades;
- Definir aplicabilidade;
- Gerar assinatura física e/ou eletrônica do termo de ciência;
- Deixar claro que é a empresa que detém a propriedade dos recursos, bem como direitos autorais das criações e demais proteções de ativos intangíveis;
- Reforçar o dever de confidencialidade e sigilo;
- Determinar a possibilidade de processo disciplinar;
- Determinar requisito de inserção de cláusulas específicas em contratos (se possível, atualizar contrato de trabalho para prever monitoramento);
- Prever procedimento de resposta a incidentes de SI (como coletar as provas sem cometer infração a privacidade ou crime de interceptação;
- Tratar da questão da mobilidade;

- Implementar vacinas legais (avisos) nas próprias interfaces gráficas." (P. 174)

Patrícia também elenca algumas regras básicas para orientar o uso dos computadores pelos trabalhadores:

1. "não abrir arquivos anexados, pois geralmente são programas executáveis que podem causar danos ao computador ou capturar informações confidenciais;
2. não clicar em links para endereços da Internet, mesmo que conste o nome da empresa ou instituição, ou, ainda, mensagens como 'clique aqui'."
3. em caso de dúvidas sobre a origem e veracidade de determinada mensagem, procurar excluir o e-mail evitando executar anexos ou acessar os links presentes em seu conteúdo;
4. em casos de contaminação por vírus ou outro código malicioso, reformatar a máquina, reinstalar totalmente o sistema operacional e os aplicativos, evitando restaurar backups antigos.
5. utilizar softwares de proteção (antivírus, anti-spam, anti-spyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas;
6. não emprestar sua senha de e-mail, de Internet, de rede da empresa em hipótese alguma;
7. duvidar do perfil de pessoas que se comunicam, em ambientes não seguros e anônimos, como Orkut, Messenger, blogs, chats, evitando clicar e abrir imagens, principalmente;
8. denunciar na delegacia de crimes eletrônicos, bom como também em sites especializados, como o 'www.denunciar.org.br'".

OBRAS CONSULTADAS

Consulta de legislação no link <planejamento.gov.br/conlegis/legislacao>

Consulta processual no site www.tst.jus.br: Recurso de Revista de n.º 625-74.2011.5.09.0001, Agravo de Instrumento em Recurso de Revista de n.º 5078-36.2010.5.06.0000, AIRR-1542/2005-055-02-40.4.

Da Silva, Ronaldo Pedroso e Cristiano Alvarenga: A Internet como instrumento da aldeia global - Revista da Católica, Uberlândia, v. 1, n. 2, p. 140-148, 2009, disponível em: <catolicaonline.com.br/revistadacatolica>

HOUAISS, Antônio. Dicionário Houaiss da Língua Portuguesa. Co-autores Mauro de Sales Villar e Francisco Manoel de Mello Franco. 1ª edição. Rio de Janeiro-RJ: Objetiva, 2001.

REPÚBLICA FEDERATIVA DO BRASIL
ORDEM E PROGRESSO

UNIBAN
UNIVERSIDADE BANDEIRANTE
DE SÃO PAULO

O Reitor da Universidade Bandeirante de São Paulo, no uso de suas atribuições
e tendo em vista a conclusão do curso de Sistemas de Informação,
em 22 de dezembro de 2009, confere o título de Bacharel em Sistemas de Informação a

Fabiano Aparecido de Oliveira

Nacionalidade: Brasileira — Natural do Estado de São Paulo

Nascido em 23 de outubro de 1975 — R.G. n.º 25295340X

e outorga-lhe o presente Diploma, a fim de que possa gozar de todos os direitos e prerrogativas legais.

São Paulo, 22 de dezembro de 2009

Coordenadora de Registro Acadêmico

Diplomado

Reitor

Prof. Dr. Heitor Pinto e Silva Filho
Reitor

Dr. Marcos Roberto Zacarin
Presidente do Conselho de Legislação e Normas Educacionais

Dr. Lúcio Flávio Cosme
Coordenador de Legislação e Normas Educacionais

Elaine Cristina Momisso Paes Leme
Coordenadora de Registro Acadêmico

Curso de Sistemas de Informação

Reconhecido pela Portaria Ministerial n.º 941/2002

D.O.U de 28/03/2002

UNIBAN - UNIVERSIDADE BANDEIRANTE DE SÃO PAULO
Centro de Registro Acadêmico
Setor de Registro de Diplomas

Diploma registrado sob n.º 063292.
Processo n.º 1004741, nos termos do Artigo 48 da Lei 9394/96.

São Paulo, 22 de dezembro de 2009

Maria de Fátima Bezerra Lopes
Auxiliar de Registro de Diplomas

De acordo.

ELAINE CRISTINA MOMISSO PAES LEME
Coordenadora de Registro Acadêmico

MARIA DE FÁTIMA BEZERRA LOPES
Auxiliar de Registro de Diplomas

FACULDADE KURIOS - FAK
CREDENCIADA PELA PORTARIA - MEC- 2.821, DE 03/10/2002

Registrado sob Nº 860 Livro 04 Folha 55 no livro de registro de documentos de cursos de complementação pedagógica conforme resolução CNE/CP Nº 5 de 2006

Programa de Complementação Pedagógica

UNIBAN
UNIVERSIDADE BANDEIRANTE DE SÃO PAULO