MBR 11
TECNOLOGIA E INFORMAÇÃO

apresenta

<h1>

TUDO QUE VOCÊ PRECISA SABER PARA ESTAR SEGURO NO MUNDO DIGITAL

</h1>

Um guia completo e simples para segurança de informações pessoais e de empresas.

<h2> APRESENTAÇÃO </h2>

Quando falamos sobre roubo de informações, invasões a computadores ou fraudes bancárias, logo nos vem à mente profissionais extremamente qualificados analisando centenas de milhares de códigos em uma cena que podia ser do filme Matrix. Mas a verdade é que existem formas muito mais simples de quebrar um sistema do que tentar encontrar brechas num código. É só usar a sua senha.

É muito comum em casos de ataques virtuais, a vítima ter colaborado entregando alguma senha ou informação útil para os invasores. Clicar em um link de um e-mail suspeito, acessar um site errado achando que é verdadeiro ou instalar um programa perigoso são exemplos de ações que o usuário pode fazer e, sem perceber, ajudar na invasão. Por outro lado, não adianta ficar com medo de usar a Internet, pois hoje é inevitável para qualquer empresa aproveitar os benefícios que a tecnologia traz. Então como saber se o cavalo de madeira tem ou não soldados infiltrados?

Pensando nisso, é muito importante para nós da MBR11 que todo mundo tenha conhecimento suficiente para identificar ameaças na rede e saber como se proteger. Baseado em pesquisas de boas práticas, nossa experiência e nosso know how técnico, elaboramos essa cartilha como um guia definitivo para sua segurança na rede. Ele foi escrito para ser didático, sem aquela parte técnica chata e complicada. Aqui vamos explicar as pequenas ações que te ajudam a se proteger ao mesmo tempo em que explicamos as principais ameaças. Crie novos hábitos e leve-os adiante em casa ou na sua empresa, e aproveite uma vida digital mais segura.

EQUIPE MBR11

CONCEITOS BÁSICOS 4
SENHAS 5
COOKIES 5
REDE PÚBLICA E PRIVADA 6
URL, LINK E DOMÍNIO 6

AMEAÇAS COMUNS 7
E-MAILS FALSOS 8
PROGRAMAS MALICIOSOS 10
ANÚNCIOS FALSOS 11
COMPRAS PELA INTERNET 12

PROTEÇÃO 13
COMPORTAMENTO 14
ANTIVÍRUS, PROXYS, FIREWALLS E OUTROS AJUSTES 16
POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO 18

CUIDADOS ADICIONAIS NO CASO DE EMPRESAS 20

CONCLUSÃO 22

QUER SABER MAIS? 23

SOBRE A MBR11 24

<h2>CONCEITOS BÁSICOS</h2>

Antes de continuar, precisamos ter certeza de que você conhece alguns termos que vamos utilizar. Entender como essas coisas funcionam vai te ajudar em muito a perceber ameaças novas assim que surgirem.

SENHAS

Pode parecer óbvio que é importante manter sua senha segura, mas é surpreendente a quantidade de usuários que esquecem a própria senha ou não se preocupam com ela. Dependendo da situação, do site ou sistema que você estiver usando, você vai precisar de uma senha para provar sua identidade. Assim como no banco você não daria sua senha para estranhos, evite criar uma senha muito simples que possa ser descoberta facilmente ou usar a mesma senha para diversos sites. Ao longo desse material, daremos mais dicas sobre boas práticas com senhas.

COOKIES

Cookies são pequenos arquivos que um site salva no seu computador. Imagine que você acessa o seu e-mail. O site vai pedir sua senha para só então mostrar o conteúdo. Se você fechar e abrir novamente o navegador, seu e-mail ainda pode estar aberto. Mas como o site sabe que é você de novo? Por causa dos cookies. Eles servem para muitas coisas. Se você entra num site de compras e vê, por exemplo, uma viagem para o Rio de Janeiro, o site de compras pode salvar um cookie dizendo que você pesquisou por isso e, quando voltar ao site, ele pode te avisar se essa viagem está em promoção. Algumas pessoas se preocupam com sua privacidade por causa de cookies, pois outros sites podem saber se você pesquisou por viagens para o Rio. Por isso, deve-se manter um certo cuidado com os sites que você acessa para evitar um uso indevido dos cookies.

REDE PÚBLICA E PRIVADA

Quando conectam-se diversos computadores chama-se isso de rede. Essa rede é privada quando todos os computadores que a acessam são controlados. É o caso de uma empresa que tem apenas os próprios computadores conectados e a rede é protegida com senha. Já as redes públicas podem ser acessadas por qualquer um. Normalmente, redes privadas são mais seguras, pois a chance de alguém com más intenções estar conectado é menor. Mas de qualquer forma, as mesma técnicas de prevenção são válidas para ambos os casos.

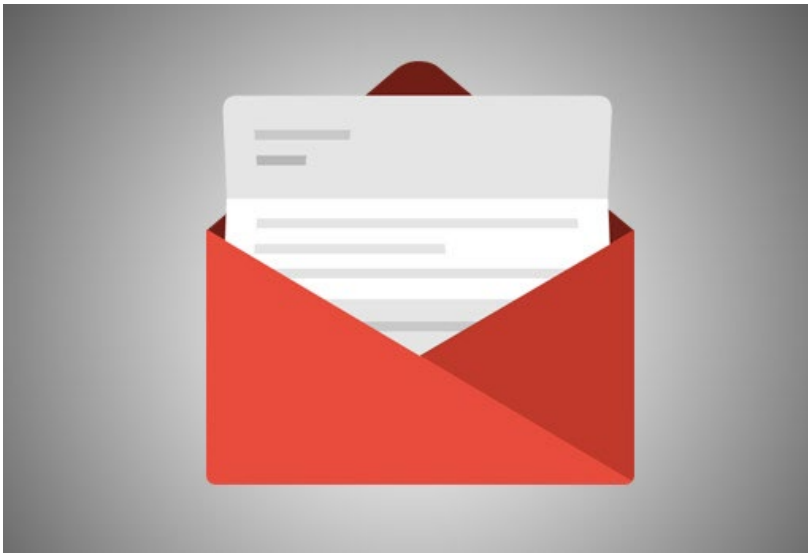
URL, LINK E DOMÍNIO

Todo site precisa de um "nome". Essa é a forma que você vai usar para encontra-lo e identifica-lo. Esse "nome" é o domínio e ele normalmente é escrito como www.exemplo.com.br. Se você quer acessar um site você precisa digitar o "nome" do site no navegador para ele saber aonde você quer ir, mas dentro do site, você pode ir para várias páginas, como a página da empresa ou uma página de contato. Então por isso existe a URL[1], que é o endereço completo da parte do site que você quer acessar, que pode ser http://www.exemplo.com.br/pagina_de_exemplo. Se você reparar na barra do navegador, você sempre verá a URL em que você está. Já o link, é um elemento (seja um texto, uma imagem ou um botão) em que você clica e é redirecionado para uma URL. É importante você entender a diferença, porque o domínio pertence ao site. Se você estiver em um domínio estranho, provavelmente o site é falso ou perigoso. Antes de clicar em um link também é importante verificar para qual URL você será direcionado.

[1] Do inglês, "Uniform Resource Locator", que significa "Localizador Padrão de Recursos".

<h2>AMEAÇAS COMUNS</h2>

Neste capítulo selecionamos as principais ameaças a que uma pessoa está exposta. Mas não precisa se desesperar, leia com a atenção que vamos ensiná-lo como se proteger.



E-MAILS FALSOS

Nesse golpe clássico, envia-se um e-mail falso para a vítima alegando-se ser alguma empresa como um banco por exemplo. O principal objetivo é o roubo de dados como nome, CPF, conta e senhas ou a instalação de programas maliciosos.

Com o roubo da senha de bancos, o prejuízo financeiro pode ser altíssimo. Com posse das suas informações, qualquer um pode se passar por você e acessar sistemas. Além disso, com programas maliciosos ele pode usar a sua máquina para fazer transações. Tudo isso sem você perceber.

O formato mais comum **consiste em um e-mail falso muito parecido com um verdadeiro**, às vezes com o logotipo, cores e a identidade da empresa de verdade. Ele é enviado para uma lista de pessoas aleatórias na esperança de que alguém clique. O e-mail costuma usar uma linguagem formal, simulando alguma marca ou pessoa, e às vezes usa palavras difíceis para dificultar o entendimento de seu objetivo e é comum haver erros de português. O padrão é uma mensagem com alguma desculpa para a pessoa clicar no link que direciona para uma página falsa ou para o download de algum programa malicioso.

EXEMPLO

Veja no exemplo como o e-mail aparenta ser real. Nesse caso, o link é falso e provavelmente vai te levar a instalar programas maliciosos. Em caso de dúvidas, entre em contato com quem aparentemente enviou o e-mail antes de tomar qualquer ação.

BANCO
DE EXEMPLO

Prezado(a),

Informativo Banco de Exemplo S/A

O Banco de Exemplo vem por meio deste, informar que seu dispositivo de segurança (iToken, Cartão de Segurança) encontra-se desatualizado com nosso sistema.

A atualização é obrigatória para clientes Banco de Exemplo Empresas, e deve ser realizada até o dia 11/03/2015, caso contrário seus acessos serão temporáriamente bloqueados (Caixas Eletrônicos, Internet Banking e Bankfone), e será cobrada uma taxa adicional de R$ 34,90 para o envio de um novo dispositivo de segurança.

*A atualização ocorrerá em ambiente seguro com o Guardião 30 horas.

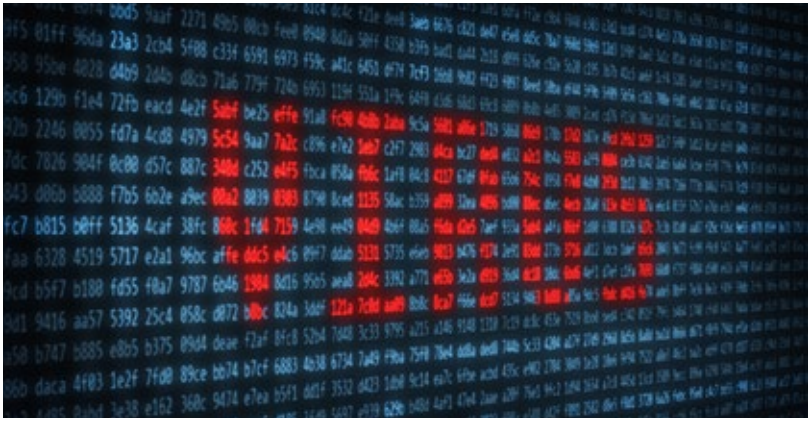
Para dar início clique no link abaixo:

https://www.bancoexemplo.com.br/seguranca/atualiza.php

Atenciosamente, Banco de Exemplo

DICA IMPORTANTE

Assim como e-mails, um golpe parecido é o de sites falsos. Para se proteger, certifique-se que você está no domínio ou na URL correta do site que você quer acessar.



PROGRAMAS MALICIOSOS

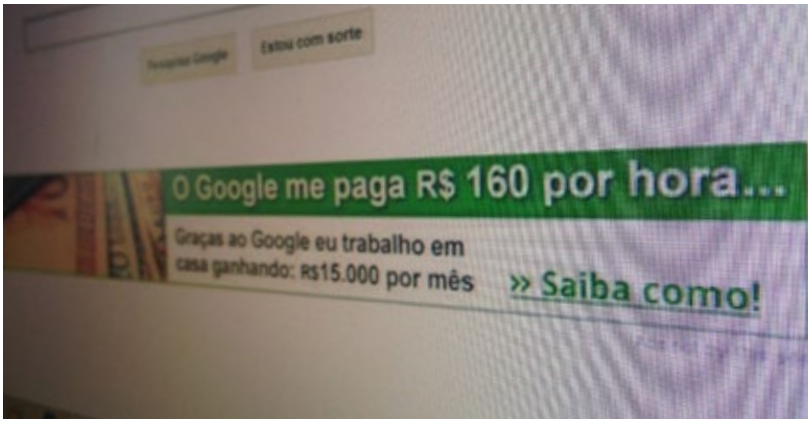
Os programas maliciosos são popularmente conhecidos como vírus. Na verdade existem vários tipos de programas com diversas finalidades diferentes. Os tipos são diversos, vírus, malwares, adwares, rootkits, bots, spywares, trojans... Mas as ações maliciosas mais comuns são a alteração ou remoção de arquivos, o consumo de recursos, o roubo de informações, instalação de outros códigos maliciosos, o uso do computador para enviar e-mails falsos ou inconvenientes e até para fazer ataques na Internet.

Além do roubo de informações, o dono da máquina infectada pode perder arquivos e desempenho do equipamento. Dependendo do tamanho da infecção e sua complexidade, a única solução pode ser a formatação do equipamento, o que nem sempre é algo conveniente a se fazer.

Existem algumas formas comuns de infecção. Se você abrir um e-mail ou site falso, é possível que essas ameaças possam ser instaladas em seu computador. Elas também podem vir infiltradas quando você tentar instalar outros programas. Por fim, pode ser que você já tenha um programa malicioso instalado e ele te leve a instalar outros acidentalmente.

DICA IMPORTANTE

Preste atenção na hora de instalar programas, ou peça ajuda de alguém experiente. É comum que mesmo programas de origens relativamente confiáveis tragam junto programas indesejáveis e você pode aceitar instalá-los sem perceber.



ANÚNCIOS FALSOS

Comuns em sites suspeitos, anúncios falsos podem induzir você a acessar sites e baixar programas maliciosos. Apesar de muito associados a sites de pornografia e de downloads piratas, alguns programas maliciosos podem trocar anúncios reais por anúncios falsos fazendo sites confiáveis exibirem anúncios suspeitos.

Esses anúncios costumam promover coisas improváveis, como "ganhe dinheiro sem trabalhar" ou "você foi sorteado e ganhou um prêmio". Sempre duvide de grandes recompensas ou promessas vazias. Também estranhe ameaças. "Você está desprotegido" ou "foram detectadas ameaças, instale o módulo de segurança aqui". Irônico clicar nesse link e instalar uma ameaça, não? O mesmo serve para conteúdo adulto de origem duvidosa.

DICA IMPORTANTE

Desconfie. Promessas fáceis ou ameaças vazias não merecem atenção. Na dúvida, clique apenas em anúncios de marcas ou lojas que você conhece e confia.

COMPRAS PELA INTERNET

Compras online são polêmicas por natureza, mas em geral não há o que temer, desde que sejam tomadas as devidas precauções. Existem pessoas mal intencionadas que criam lojas falsas com ofertas aparentemente vantajosas, mas que visam apenas uma fraude.

O perigo está em informar dados pessoais como nome, CPF, endereço e cartão de crédito. Com esses dados, o infrator pode, além de lhe roubar, se passar por você e cometer outros crimes.

No caso de lojas virtuais, a melhor prevenção é a pesquisa. Antes de tudo avalie se não é um caso de site falso tentando se passar por uma loja real. Se realmente não for, estude a loja verificando se há reclamações graves em sites como o Reclame Aqui ou o consumidor.gov.br. Pesquise bastante, em outros sites, redes sociais, tente encontrar pessoas que atestem a qualidade da loja. Não encontra outras informações na Internet? Preocupe-se e evite.

DICA IMPORTANTE

Essa loja possui um produto com preço muito inferior ao de qualquer outra loja? Fique atento, pois esses descontos exagerados podem ser falsos. Se você ver um produto que normalmente custa R$ 1.000,00 por apenas R$ 99,99, o vendedor teria uma margem de lucro muito pequena, se não negativa. Na dúvida, repense sua compra.

<h2>PROTEÇÃO</h2>

Ok, você já conhece as ameaças. Agora, o que fazer para estar protegido? As dicas a seguir são fundamentais para sua segurança na rede.

COMPORTAMENTO

Como já abordamos, não adianta ter o melhor antivírus, uma infraestrutura completa e segura de rede e os melhores técnicos à disposição. Seu comportamento pode ser decisivo na hora de se proteger contra ameaças digitais.

Algumas atitudes que podem te ajudar a estar protegido:

- Cuidado ao usar a Internet em **computadores públicos**. Se for inevitável, nunca esqueça de sair do seu e-mail, sua rede social ou qualquer outro site que tenha aberto;
- Atente para quais **informações pessoais você divulga na Internet.** Mesmo redes sociais ou cadastros em sites podem acabar sendo um prato cheio para ataques virtuais;
- Apenas **clique em links ou instale programas** que vieram de fontes seguras e verifique se não está sendo enganado;
- Desconfie de qualquer **solicitação de dados** seus que venha pela Internet, mesmo que seja de empresas ou pessoas confiáveis;

- **Crie senhas seguras.** Nada de 123456 ou data de aniversário. Tente misturar letras, números, maiúsculas, minúsculas, símbolos e até letras acentuadas. A chance de alguém descobrir sua senha diminuirá drasticamente. Também evite repetir a mesma senha em diversos lugares;
- **Coloque senhas no computador, celular e tablet.** Algumas pessoas acham mais conveniente deixar o equipamento sem esse tipo de segurança, mas é fundamental manter suas informações protegidas;
- **Operações confidenciais?** Prefira fazer isso em seu computador pessoal. Pagamento de contas, operações bancárias ou compras online são mais seguras se forem sempre realizadas no mesmo equipamento (desde que ele esteja adequadamente seguro);
- **Preços muito abaixo do mercado** podem ser uma fraude. Atenção redobrada nesses casos;
- No caso de compras online, existem serviços como o PagSeguro ou o PayPal que lhe dão **garantias da integridade daquela loja.** Fique atento a esses sinais;
- **Atenção também para aplicativos.** Ameaças para dispositivos móveis tem crescido bastante, então use apenas lojas de aplicativos confiáveis e verifique que permissões você dá para cada aplicativo.

Além de tudo isso, também é importante você se preocupar com outras pessoas que usam o seu dispositivo, compartilhem sua rede ou trabalhem contigo. Ensine a essas pessoas como se proteger e monitore novos usuários até que eles tenham certa experiência.

E também **não ache que você é muito insignificante para sofrer um ataque.** Esse tipo de ação criminosa é feita em escala com o máximo de pessoas possível para que alguns poucos caiam no golpe e faça valer a pena. Mesmo seu computador não tendo dados como cartão de crédito ou senhas, até sua lista de contatos pode ser útil para os criminosos.

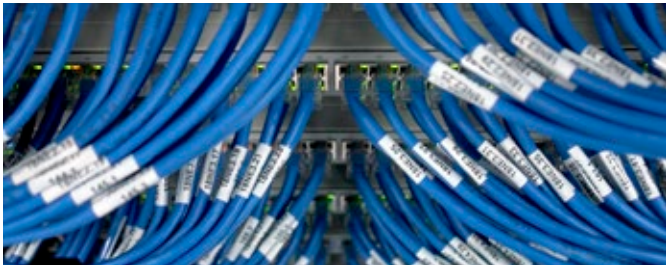
ANTIVÍRUS, PROXYS, FIREWALLS E OUTROS AJUSTES

Mais uma vez: de nada adianta ter recursos avançados de segurança se não houver **cuidados por parte do usuário**. Dito isso, qualquer ajuda é bem-vinda. Existe uma gama de possibilidades técnicas que podem ajudar você a proteger suas informações.

Um **antivírus** é, talvez, a ferramenta mais popular para proteção contra softwares maliciosos. Ele é um programa que pesquisa sua máquina em busca de vírus ou outras ameaças. É bastante útil para evitar ameaças mais comuns.

Outra ferramenta útil é o **firewall**. Ele é um programa que cria um "muro" entre o computador e a Internet, impedindo todas as conexões a não ser aquelas permitidas. Isso evita que vírus ou invasores acessem seu computador através de conexões ocultas.

Para empresas, que normalmente têm uma estrutura maior, vale a pena instalar servidores dedicados para o firewall e para proxys. O **servidor de proxy** é um equipamento intermediário que monitora tudo que os computadores tentam acessar da Internet e pode bloquear acessos indesejáveis como sites perigosos ou falsos, além melhorar a conexão.

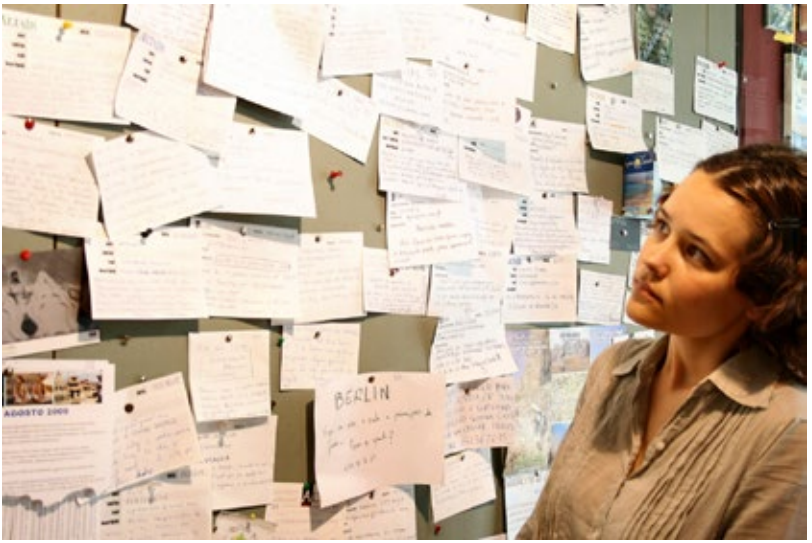


Não se esqueça de manter seus **sistemas e softwares constantemente atualizados**. A maior parte das atualizações serve justamente para corrigir falhas que permitiam que um invasor aproveitasse para se instalar no equipamento. O mesmo vale para firmwares de equipamentos, que são os programas específicos instalados diretamente no equipamento como roteadores ou computadores.

Para evitar que você perca dados ou arquivos importantes, lembre-se de fazer cópias de segurança deles. Existem diversas opções interessantes no mercado de **ferramentas de backup**. Também vale lembrar que **programas piratas** normalmente não têm suporte às atualizações ou podem vir já com vírus, portanto não vale a pena correr esse risco.

DICA IMPORTANTE

Alguns equipamentos como roteadores **vem de fábrica com configurações padrões, incluindo senhas**. O problema é que muitas pessoas esquecem ou não sabem que precisam mudar essa senha. Se alguém conseguir acessar sua rede, e os dispositivos estiver com a senha padrão, você corre o risco de ter suas informações roubadas.



POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Essa dica é específica para empresas. Como são várias pessoas usando computadores e recursos tecnológicos, é importante que todos sejam treinados e saibam **o que pode e o que não pode ser feito.** Essa lista de regras é chamada de Políticas de Segurança da Informação. Essas políticas devem ser elaboradas e repassadas para um novo colaborador desde seu primeiro dia de trabalho.

Um exemplo de ação prevista pelo PSI é o controle de acesso. Quando há várias pessoas na mesma rede, é comum haver o compartilhamento de pastas e arquivos. Mas que pessoas têm acesso a quais arquivos? Alguém de um departamento comercial, por exemplo, não precisa acessar todos os arquivos da equipe de produção, e vice-versa. Deve-se criar, então, regras de acesso que dão permissões específicas para cada usuário tanto para acessar arquivos quanto para alterar configurações do equipamento.

A PSI serve para definir regras desde o uso de e-mails, de sites, backups, dispositivos móveis, identificação, entre outros aspectos. Aconselhamos o acompanhamento de um profissional na hora de desenvolver sua PSI, mas não é algo obrigatório. Por mais simples que sejam, qualquer regra, desde que devidamente apresentada e aceita, é válida.

É importante mencionar também, que uma boa Política de Segurança da Informação prevê aspectos legais de crimes virtuais e ajuda a evitar que situações indesejadas aconteçam entre empresa e colaboradores.

DICA IMPORTANTE

Se sua empresa for pequena e não quiser ser muito burocrática, tenha em mente que alguns aspectos pontuais devem ser ao menos apresentados para os colaboradores. Avise se eles podem ou não abrir e-mails pessoais ou usar pendrives e HDs externos, e certifique-se de dar todo tipo de acesso a arquivos necessários bem como revogar esses acessos no fim de um contrato.

CUIDADOS ADICIONAIS NO CASO DE EMPRESAS

Empresas precisam de atenção dobrada nesse caso. Em muitos negócios diferentes, a informação é o ativo mais precioso do negócio e perder essas informações ou tê-las em mãos erradas pode ser desastroso para o negócio.

NEGLIGÊNCIA HUMANA E ERROS DE SISTEMA PODEM CAUSAR PERDAS DE ATÉ R$ 9,74 MILHÕES PARA EMPRESAS.

Temos inúmeros casos para exemplificar. Em 2013 a Symantec e o Ponemon Institute divulgaram uma pesquisa que revela que **negligência humana e erros de sistema** são responsáveis por dois terços dos vazamentos de dados.

MBR 11
TECNOLOGIA E INFORMAÇÃO

Nesse caso, dois devem ser os focos principais das empresas: garantir treinamento adequado de seus colaboradores no dia-a-dia da empresa e assegurar que seus sistemas estão protegidos e devidamente configurados. Afinal, segundo esse mesmo estudo, **o custo para um vazamento de dados fica entre R$ 230 mil e R$ 9,74 milhões** que inclui gastos com perda de clientes, reputação e de relacionamento.

E, como já mencionado anteriormente, é um erro achar que só porque o negócio é pequeno, tem poucos computadores ou funcionários, que ele não está sujeito às ameaças. **Pequenas e médias empresas normalmente são mais inseguras** e é mais fácil fazer ataques em volume para que algumas deem um retorno interessante para os criminosos.

DIVULGAR ESSE CONHECIMENTO É O PRIMEIRO PASSO PARA TORNAR SUA EMPRESA MAIS SEGURA.

Então pensando nisso, você ler esse próprio material é um primeiro passo importante para pensar na segurança de sua empresa. **Divulgue esse conteúdo dentro de sua empresa** e certifique-se que essas atitudes sejam seguidas com rigor. Mas além disso, é importante ter certeza de que seus sistemas estão protegidos e devidamente configurados.

Isso nos leva a um questionamento. **Qual o nível de atenção que você dá para a Tecnologia da Informação (TI) de sua empresa?** Normalmente empresas maiores possuem um departamento dedicado para isso, mas empresas menores não conseguem arcar com os custos e, se problemas aparecem, elas são obrigadas a resolver questões tecnológicas sozinhas ou com a ajuda de terceiros que podem não ser confiáveis ou podem não ser a melhor solução para o seu negócio.

A FUNÇÃO DO TI É GARANTIR QUE TUDO FUNCIONE COMO DEVERIA PARA A EMPRESA TER SUCESSO.

Portanto sempre certifique-se da procedência de quem dá assistência para sua empresa. Nesse caso, uma alternativa interessante são contratos fixos de outsourcing de TI, onde mesmo uma pequena empresa pode terceirizar a responsabilidade pela tecnologia dela com profissionais qualificados e ter sempre alguém atento para garantir que esses processos de segurança são seguidos.

<h2> CONCLUSÃO </h2>

Os computadores e a Internet surgiram na nossa vida há pouco tempo. Sem dúvidas, são ferramentas muito interessantes para nos dar agilidade e simplificar processos, mas, infelizmente, sendo tão rápidas, podemos esquecer de discutir se a nossa forma de interagir com informações virtuais é a mais adequada.

É importante ressaltar que as informações apresentadas aqui servem apenas como uma orientação inicial para evitar os problemas mais comuns, mas é um excelente ponto de partida para estar mais seguro na Internet.

Sua missão, a partir daqui, é entender e difundir esses conceitos, ajudando pessoas um pouco menos experientes a garantir sua própria segurança ao lidar com arquivos digitais.

Aproveite uma vida digital mais segura!

QUER SABER MAIS?

CARTILHA DE SEGURANÇA PARA INTERNET DO CERT.BR

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) criou uma cartilha bastante didática que aprofunda, sempre de forma didática, alguns dos conceitos explorados aqui.

http://cartilha.cert.br/

CALCULADORA DE RISCOS DE VIOLAÇÃO DE DADOS DA SYMANTEC

Criada pela Symantec, essa calculadora estima qual o custo e o impacto que uma violação de dados teria no seu negócio.

http://www.databreachcalculator.com/

BLOG DA MBR11

Criado para ajudar donos de empresas e gestores, o blog da MBR11 aborda além de segurança da informação, outras informações úteis para empresas conseguirem mais com sua própria estrutura de TI.

http://www.mbr11.com.br/blog/

MBR11
TECNOLOGIA E INFORMAÇÃO

SOBRE A MBR11

A MBR11 oferece soluções de TI para empresas. Nosso objetivo é resolver os problemas de tecnologia de empresas, seja na manutenção de computadores rápida e inteligente, desenvolvimento de sistemas ou consultoria.

Conheça nosso blog e aprenda tudo que você precisa saber sobre tecnologia para sua empresa.

ENTRE EM CONTATO

GOSTOU? COMPARTILHE:

Imagens
Unsplash/Luis Llerena
Flickr/download.net.pl
Flickr/Yuri Samoilov
Reprodução/Wiliam Koester
Flickr/Maria Elena
Unsplash/William Iven
Pixabay/pixelcreatures
Flickr/Andrew Hart
Flickr/Jorge Franganillo
Unsplash/Benjamin Child