CeTI-RP / STI

USP

Boas práticas de segurança para usuários de informática (versão 2023)

Expediente

Universidade de São Paulo
Reitor
Prof. Dr. Carlos Gilberto Carlotti Junior

Vice-Reitora
Profa. Dra. Maria Arminda do Nascimento Arruda

Campus de Ribeirão Preto
Prefeita do Campus
Profa. Dra. Léa Assed Bezerra da Silva

Superintendência de Tecnologia da Informação
Superintendente
Prof. Dr. João Eduardo Ferreira

Centro de Tecnologia da Informação de Ribeirão Preto
Diretor
Prof. Dr. Ildeberto Aparecido Rodello

Colaboradores Técnicos:
Clélia Camargo Cardoso (ccardoso@usp.br)
Analista de Sistemas CeTI-RP/STI
Marcelo Contin (mcontin@usp.br)
Analista de Sistemas CeTI-RP/STI

Thiago Merenda (tmerenda@eerp.usp.br)
Analista de Sistemas da Seção Técnica de Informática EERP-USP

Robson Eisinger (eisinger@usp.br)
Analista de Sistemas CeTI-SP/STI

Claudia Helena Bianchi Lencioni (claudia@usp.br)
Atd. CeTI-RP/STI

Apoio
IEA-RP

Diagramação
João Henrique Rafael

Sumário

1 - Introdução

“Todos somos responsáveis de tudo, perante todos” (*Dostoievski*)

A todo momento vemos notícias de novas ameaças cibernéticas. A maioria acusa os *hackers* por comprometer sistemas e causar prejuízos às instituições.

O que não é falado, contudo, é que normalmente o que permite que os *hackers* invadam ou causem algum estrago é nossa ação inadvertida como usuário.

Estatísticas apontam que a ação do usuário é a principal causa do comprometimento dos sistemas de informação nas instituições, podendo ser atribuída a duas deficiências:

- **Falta de treinamento** com o desconhecimento das consequências que sua ação inadvertida pode causar ao sistema;

- **Falta de comprometimento** com o uso irresponsável dos recursos da instituição.

Como usuários, é nosso dever zelar pelo bom uso dos recursos computacionais que usufruímos em nossa instituição, sendo o propósito da presente cartilha a conscientização dos principais riscos presentes na Internet, bem como esclarecer as consequências do mau uso desses recursos.

crédito: pixabay

2 - Impacto de nossas ações como usuários

Nem sempre temos consciência do impacto que causamos no mundo a nossa volta, acreditando que nossas ações afetam apenas a nós mesmos.

Quando instalamos um *software* pirata ou compartilhamos nossa senha, estamos na verdade fazendo um convite ao perigo.

A instalação de *softwares* piratas, não se resume apenas ao seu uso não autorizado. Por não ter suporte, os *softwares* piratas são mais passíveis de *bugs* que podem comprometer o bom funcionamento do sistema.

Indo além disso, para burlar as proteções contra pirataria, esses *softwares* costumam ter alterações em seu código, e em alguns casos são introduzidos mecanismos que permitem o acesso não autorizado à máquina por *hackers*.

Em outras palavras, o uso de *software* pirata compromete o computador, e uma vez dentro de nossa rede, é apenas um passo para invadir as demais máquinas e ter acesso a um sistema crítico da instituição.

Outra questão importante é o compartilhamento de senhas. Cada um de nós é responsável pelas senhas das contas que administramos e é nosso dever entender que:

- Ao compartilhar a senha com terceiros, não estamos "terceirizando" a responsabilidade pela mesma. Em caso de invasão ou mau uso, somos os únicos responsáveis pelas contas que administramos, arcando com as consequências. Ao compartilhar nossa senha, apenas aumentamos o risco de invasão ou comprometimento e

- Nenhum administrador solicita (ou deve solicitar) senha por e-*mail,* esse tipo de *e-mail* tem como propósito obter acesso a uma conta para fazer uso da mesma com fins maliciosos.

Já que mencionamos *e-mails* maliciosos, nem sempre eles são explícitos, passando-se como uma mensagem do administrador de sistema ou um falso aviso de segurança, muitas vezes solicitando usuário e senha.

Também é importante tomar cuidado com os *links* que recebemos por *e-mail*. Muitos *hackers* e/ou *spammers* utilizam propaganda de uma marca ou companhia conhecida, nos seduzindo com alguma promoção ou oferta interessante, e uma vez que clicamos no *link*, corremos o risco de instalar inadvertidamente um *software* malicioso em nosso sistema.


crédito: pixabay

Assim, é recomendado sempre confirmar a procedência da mensagem.

Outro ponto controverso é o uso de recursos computacionais da instituição para fins pessoais. Seja usando um *pendrive* ou dispositivo similar, ou baixando os arquivos. Dois aspectos devem ser considerados:

- Os arquivos podem estar contaminados por um *malware* e comprometer o sistema. Por melhores que sejam as ferramentas de antivírus, nem sempre elas estão preparadas para combater as últimas versões das ameaças cibernéticas. *Hackers* têm usado legendas de vídeo para propagar vírus, por exemplo, e existem diversas variantes de ataques usando documentos do Word e PDF para se propagar sem o conhecimento dos usuários e

- O consumo de recurso, como espaço em disco e o acesso à Internet para fins pessoais pode prejudicar o serviço de todos os demais usuários, ainda mais com o aumento no uso dos chamados *Desktops* Virtuais, onde tudo é disponibilizado a partir da nuvem.

Os recursos costumam ser compartilhados ou usar uma rede comum, e em muitos casos a lentidão no serviço fornecido pode ser consequência do mau uso de um ou mais usuários e não propriamente um problema do serviço fornecido.

A própria questão da imagem da instituição precisa ser considerada, por exemplo, ao propagar correntes e notícias usando nossas contas de *e-mail* institucionais, sem verificar sua veracidade, precisamos lembrar que somos representantes de nossa instituição.

Assim, temos que ter cuidado com o tipo de informação que repassamos. Isso também vale quando compartilhamos informações confidenciais, se não houver certeza se algo é confidencial e restrito ao ambiente de trabalho, não deve ser compartilhado.

3 - Recomendações

É importante usar o bom senso e, havendo dúvida, procurar auxílio junto à Seção de Informática responsável. Assim, seguem abaixo algumas recomendações pertinentes ao uso dos recursos computacionais na instituição:

• Evitar sempre que possível o uso da estação de trabalho para fins particulares;

• O *e-mail* corporativo deve ser usado apenas para as atividades que fazem parte das atribuições da instituição. Assim, se ela for uma instituição de ensino, como a Universidade de São Paulo, seu uso é restrito para fins acadêmicos e de pesquisa, ou para o exercício de atividades profissionais. Para questões particulares, fazer uso de *e-mail* pessoal;

• Não deixar documentos e arquivos pessoais na estação de trabalho ou *e-mail* corporativo, pois outras pessoas podem acessar o computador, seja para manutenção ou quando o recurso for alocado para outro setor, por exemplo. Isso ajuda a manter a privacidade do usuário;

• *Backup* deve fazer parte da rotina, lembrar-se sempre de fazer *backups* regulares dos dados corporativos, como documentos, *e-mails*, contatos etc. Periodicamente lembrar-se de confirmar se o *backup* foi realizado corretamente, para garantir que as informações guardadas possam ser recuperadas para uso futuro, caso ocorra um imprevisto;

• Ter sempre na estação de trabalho um *software* antivírus e *firewall*, de preferência aqueles que são homologados pela instituição, em caso de dúvida, entrar em contato com a Seção de Informática da unidade;

• Nunca instalar *software* pirata, conforme explicado, eles podem conter código malicioso que permite acesso remoto à estação de trabalho do usuário, podendo comprometer não apenas ela, como todas as máquinas que estiverem na mesma rede;

• Evitar instalar *software* gratuíto encontrado na Internet, instalar apenas aqueles que são homologados/autorizados pela Seção Técnica de Informática e sempre de fontes confiáveis, como o site do fabricante/desenvolvedor do *software*;

• Nunca fornecer a senha de alguma conta que administre, seja a senha do computador, *e-mail* ou outro sistema, para terceiros. Se essa pessoa precisa acessar determinado recurso, isso deve ser feito a partir de sua própria conta, com a devida autorização;

• Não utilizar *softwares* de distribuição de arquivos ou P2P, aqueles que permitem que os usuários compartilhem arquivos entre si, como por exemplo Kazaa, Gnutella e BitTorrent. Estes *softwares* abrem portas para invasão e podem compartilhar arquivos contaminados, vídeos ou imagens abusivas e ainda ferir direitos autorais;

• Procurar manter-se atualizado sobre o uso consciente e seguro da Internet.

Seguem abaixo alguns links com material relevante sobre o tema:

- https://cartilha.cert.br/livro
- https://cartilha.cert.br/fasciculos/
- https://internetsegura.br/

A Superintendência da Tecnologia da Informação disponibiliza uma cartilha para usuários que trata sobre a utilização de *e-mails* de forma segura: http://cetirp.sti.usp.br/wp-content/uploads/sites/47/2016/02/Cartilha_Boas_Praticas-CeTIRP-USP.pdf

Algumas normas sobre a utilização dos recursos computacionais da universidade e Código de Ética, podem ser encontrados no link abaixo: https://www.sti.usp.br/legislacao/normas/


crédito: pixabay

4 - Incidentes de segurança

Um incidente de segurança é todo evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

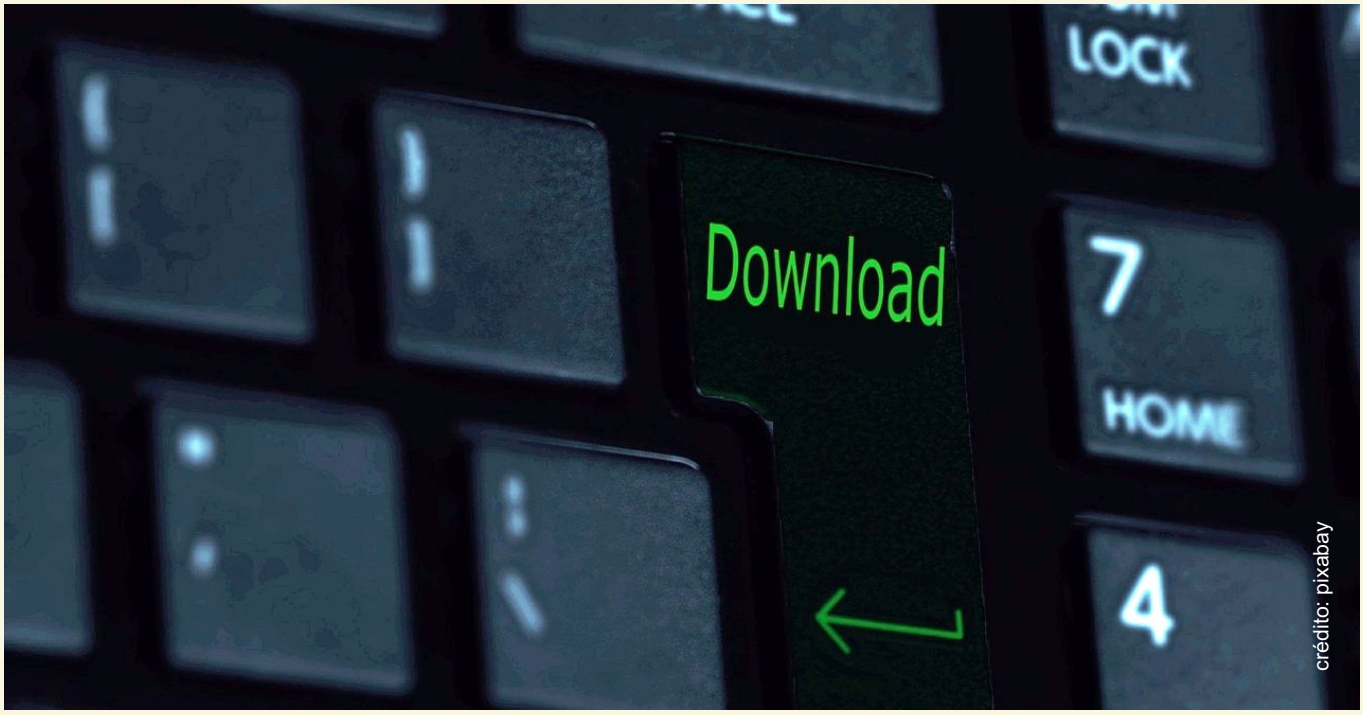
Em geral, toda situação onde uma entidade de informação está sob risco é considerado um incidente de segurança. Ele pode ser o resultado de uma violação de segurança, por exemplo, um acesso não autorizado a informações ou um site retirado do ar por ação de um *hacker*.

Os incidentes de segurança devem ser reportados à equipe responsável pela segurança da informação da instituição. Na Universidade de São Paulo, esse papel é desempenhado pelo Grupo de Segurança em Tecnologia de Informação (GSeTI), que trabalha como um Centro de Tratamento e Resposta a Incidentes de Segurança (CSIRT, em inglês), centralizando todos os incidentes de segurança da Universidade, repassando-os para que os responsáveis tomem a devida ação, retornando com a medida tomada para solucioná-la. Todo incidente de segurança deve ser notificado para:

- **Site oficial do GSeTI:**
https://www.security.usp.br/
- **Contatos:**
security@usp.br / abuse@usp.br

crédito: pixabay

5 - Vulnerabilidade dos softwares



Softwares, tanto sistemas operacionais quanto aplicativos, podem conter vulnerabilidades exploradas pelos *hackers*.

As empresas produtoras de *software* disponibilizam as correções para que os administradores e usuários possam atualizar seus sistemas.

Cada vulnerabilidade pode permitir dezenas de ocorrências de incidentes de segurança. Seguem algumas causas de ocorrências em falhas de *software*:

- Erros na instalação e configuração podem abrir portas para ataques e
- Bugs em aplicativos e sistemas operacionais bem como *softwares* piratas com códigos maliciosos embutidos podem contaminar sistemas operacionais e aplicativos instalados.

Os usuários devem seguir as recomendações:

- Não instalar *software* sem a autorização de técnico de informática responsável;
- Utilizar versões gratuitas de aplicativos somente quando baixados diretamente do site da empresa que fabrica o *software*;
- Utilizar versões *web* de aplicativos e
- Não instalar aplicativos anexados em *e-mails* ou baixados das redes sociais.

6 – Malware (malicious software)

Malware é um termo utilizado para descrever diversos tipos de *softwares* maliciosos como *trojans, phishing, spyware* , etc., que vão além dos conhecidos vírus de computador.

- ## *Phishing*

Fraude pela qual o usuário é atraído e induzido a revelar informações confidenciais como senhas, dados bancários, cartão de crédito, e o direcionamento para sistemas falsos com aparência de sistemas legítimos e de *e-mails* contendo formulários.

Foi criada a lei 12.737/12 de 30/11/2012, artigo 154, que dispõe sobre a tipificação criminal de delitos informáticos, bem como invadir dispositivo com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita, além de estabelecer punições específicas. Todos os dias, milhões de ameaças virtuais são espalhadas pela Internet. Boa parte desse montante pode ser classificada como *phishing*. Essa prática, como o nome sugere ("*phishing*" em inglês corresponde a "pescaria"), tem o objetivo de "pescar" informações e dados pessoais importantes através de *links* falsos para Receita Federal, bancos, INSS, dentre outros. Para não cair em armadilhas como essa, o usuário deve estar muito atento e prevenido, excluindo a mensagem ou verificar a autenticidade junto à Seção Técnica de Informática da unidade. Abaixo um exemplo de *e-mail phishing*:

CARO CLIENTE DE CONTA MAIL USP
Devido ao congestionamento em todas as contas USP e remoção de todas as contas desnecessárias USP, o serviço terá que fechar todas as contas não utilizadas, você precisa confirmar o seu *e-mail*, preencha suas informações de login abaixo após clicar no botão resposta, ou a sua conta será suspensa dentro de 24 horas por razões de segurança.
*ID Mail: .....
* Password: .....
* E-mail: .....
* Password: .....
* Secundária Email: .....
* Password: ..... .
* Data de nascimento: .....
* País ou Território: .....
* Profissão: .....
* TEL: .....
Depois de seguir o Registro instruções, sua conta não será interrompido e continuará como de costume.
Obrigado pela sua atenção a este pedido.
Sinceramente USP.BR equipe.

Um exemplo de *fishing* que está ocorrendo no Google Chrome é a simulação de uma pesquisa que induz o usuário a preencher um formulário com dados pessoais para concorrer a um prêmio, conforme figura abaixo nesta página.
Por isso o usuário tem que ficar sempre atento e antes de qualquer providência, procurar ajuda com a Seção de Informática da unidade.

• Vírus digital

O vírus biológico é um micro-organismo que pode infectar outros organismos biológicos. Por analogia, um vírus em Informática é um programa malicioso desenvolvido que, tal como um vírus biológico, infecta o sistema, fazendo cópias de si mesmo espalhando-se para outros computadores, utilizando-se de diversos meios.

• Worm

É um programa auto replicante, semelhante a um vírus. O vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o *worm* é um programa completo e não precisa de outro programa para se propagar.

• Cavalo de troia (*trojan*)

Difere do vírus porque não se duplica e também não contamina outros programas. São programas autônomos, camuflados em aplicativos do tipo jogos, protetores de tela e precisam ser executados para se instalar. Ao ser instalado, o *trojan* cria uma maneira de alguém entrar no computador conectado à Internet sem que o usuário perceba, permitindo que um intruso detenha o controle da máquina acessando dados e efetuando tarefas.

• Ransomware

É um tipo de *malware* que restringe o acesso ao sistema infectado e cobra um resgate em dinheiro para que o acesso possa ser restabelecido, caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados (fonte: Wikipédia). Antes restrito aos computadores pessoais, novos tipos de *ransomware*

já miram dispositivos móveis como os *smartfones* e *tablets*. Há algum tempo máquinas espalhadas pelo mundo todo sofreram ataque por um *ransomware* denominado Wannacry. A melhor precaução é o conjunto de boas práticas já citadas anteriormente, em especial fazer o *backup* dos dados, cujo acesso pode ser bloqueado pelo ataque a fim de solicitar o resgate em dinheiro. Em casos de invasão, é recomendado isolar a máquina da rede evitando o máximo de interferência quanto possível, para posteriormente tomar uma ação para resolver o problema ou identificar como a invasão foi cometida. Comunicar a ocorrência à Seção Técnica de Informática da Unidade.

Sintomas da contaminação por algum *malware*: algumas anomalias podem significar manifestação acidental ou

- Lentidão na execução de programas e perda de desempenho;

- Arquivos corrompidos ou aumento do tamanho dos arquivos executáveis ou do sistema; desaparecimento inexplicável de arquivos do disco;

- Redução de espaço livre da memória RAM;

- Surgimento de mensagens de erro estranhas ou interferências na tela durante o uso normal;

- Travamentos do teclado ou da máquina e

- Mudança na configuração de data e hora

Aos usuários, recomenda-se fortemente:

- Uma combinação de bons hábitos, uso de programa antivírus com *firewall* e atualização automática de todo *software* instalado;

- Uso de senhas difíceis de serem descobertas é uma das técnicas mais simples. A maioria dos usuários escolhe senhas que são fáceis de memorizar tais como o primeiro nome, variações do nome da empresa, etc. facilitando o acesso à máquina. Existem programas que testam exaustivamente senhas na tentativa de invasão. A senha ideal deve ser totalmente aleatória e não pode ser adivinhada com base em qualquer dado ligado ao usuário, e/ou palavra comum, devendo ser evitado o número de RG, CPF, datas de aniversário e coisas semelhantes. As senhas devem ser alteradas frequentemente e a lista

de senhas deve ser mantida em local seguro de acesso restrito;

• Fazer *backup* de todos os arquivos de dados, tendo vários jogos de *backup* com rotação periódica em mídias externas ou em nuvem;

• Evitar emprestar mídias graváveis como *pendrives* que podem retornar contaminados;

• Não executar arquivos anexados a *e-mails*, mesmo que sejam de pessoas conhecidas, pois elas podem estar com as máquinas infectadas. Em último caso, tais arquivos devem passar por verificação pelo antivírus antes de serem abertos ou executados e

• Os sistemas operacionais Linux e OS são menos vulneráveis à ação dos vírus, mas não estão totalmente livres de infecção.

crédito: pixabay

7 – Spywares e adwares

Spywares ou espiões podem ser designados como quaisquer programas ou componentes de programa que ficam intencionalmente ocultos no computador sem a permissão do usuário, tentando adquirir informações de caráter privativo e utilizando os recursos do computador.

Adwares, são programas ou *scripts* (sequência de instruções) que exibem anúncios no sistema sem serem solicitados.

Esses *malwares* são distribuídos por *trojans*, programas gratuítos ou piratas ou através da navegação na Internet pois muitos *sites* oferecem *plug-ins*, que o usuário instala inadvertidamente.

Atividades maliciosas dos *spywares* podem ser:

- Gravar os hábitos de navegação do usuário e os *sites* visitados na Internet;
- Gravar informações sobre produtos adquiridos e os gastos em compras pela Internet;
- Copiar informações sobre cartões de crédito do usuário;
- Extrair endereços de *e-mail* do usuário gravados em listas do Windows;
- Detectar senhas e outras informações confidenciais;
- Causar danos ao sistema operacional pois se utilizam de recursos do sistema (memória e processador) e
- Deixar a máquina vulnerável a ataques de *hackers*.

Recomendações e cuidados que o usuário deve ter:

- Ser seletivo com o que instala no computador. Não clicar em botões "Sim, aceito" quando instalar um *software* ou *plug-in,* sem antes pesquisar ou consultar técnico de informática da unidade;
- Ser cuidadoso com programas que mostram propagandas na tela. Caso as visualize, provavelmente estará visualizando um *spyware/adware*, e
- Usar somente *sites* de *download* confiáveis.

Na dúvida, sempre consultar a Seção Técnica de Informática da unidade

8 - Engenharia social

O termo utilizado para descrever uma ação onde um infrator tenta conseguir dados fazendo uso da ingenuidade e da confiança do usuário.

Como exemplo, podemos citar uma ligação onde o infrator informa que é um funcionário ou gerente de um determinado banco e solicita para o usuário a confirmação de sua senha e seus dados pessoais.

Chama-se Engenharia Social, pois o sucesso do ataque depende da decisão do usuário em fornecer seus dados.

9 - Antivírus

Os *softwares* antivírus além de procurarem por vírus conhecidos em um banco de dados de informações, utilizam-se de outras técnicas tentando encontrar vírus desconhecidos.

Portanto é imprescindível estar com o antivírus atualizado e ativo para que ele possa ajudar na proteção do computador.

Para qualquer evento atípico como lentidão, arquivos abrindo sozinhos, propagandas e *softwares* que não são reconhecidos é necessário abrir um chamado técnico junto à Seção Técnica de Informática da unidade para verificação do computador por um técnico.

Seguem algumas recomendações:

- A Superintendência da Tecnologia da Informação da USP disponibiliza um *software* antivírus corporativo, que pode ser obtido pelo usuário através das Seções Técnicas de Informática;

- A Microsoft também disponibiliza o antivírus Microsoft Security Essentials porém para a versão Seven não haverá mais suporte a partir de janeiro de 2020.

- Não assumir que todos os seus computadores estão livres de vírus, apenas porque um deles está. Repetir o procedimento de verificação em todos os computadores da rede local. Verificar os computadores e dispositivos móveis domésticos também;

- Não permitir que qualquer pessoa utilize o computador inserindo mídias de origem duvidosa;

- Fazer *backup* dos dados em vários conjuntos diferentes protegendo-os da ação dos vírus e desastres com o disco;

- Atualizar sistematicamente o *software* antivírus. Este procedimento pode ser habilitado para ficar automático. O *upgrade* do software incorpora novas funcionalidades e novas técnicas de remoção e detecção e

- Se um vírus for detectado, ele deve ser eliminado imediatamente, não continuar a operar a máquina e retirar o cabo de rede evitando a sua propagação, comunicar o incidente imediatamente ao técnico de informática da unidade.

10 - Firewall

O termo *firewall* significa parede corta-fogo, na Informática significa proteção contra a transmissão de dados nocivos ou não autorizados de uma rede a outra.

Um *firewall* pessoal é uma das alternativas para proteção do equipamento do usuário individualmente, atuando não na rede da organização, mas sendo capaz de controlar o acesso aos recursos, bloquear determinadas conexões, monitorar o tráfego gerado ou o que chega ao sistema, gerar regras e criar *logs* (registros) de todos os acessos ao sistema.

Algumas de suas funcionalidades:

- Ocultar o computador na Internet para que os *hackers* não o identifiquem;
- Bloquear as conexões suspeitas;
- Evitar que informações confidenciais sejam enviadas sem o conhecimento;
- Impedir o envio automático de mensagens por *e-mails;*
- Bloquear anúncios da *Web*;
- Bloquear os ataques da Internet e
- Definir quais programas podem ser conectados com segurança à Internet.

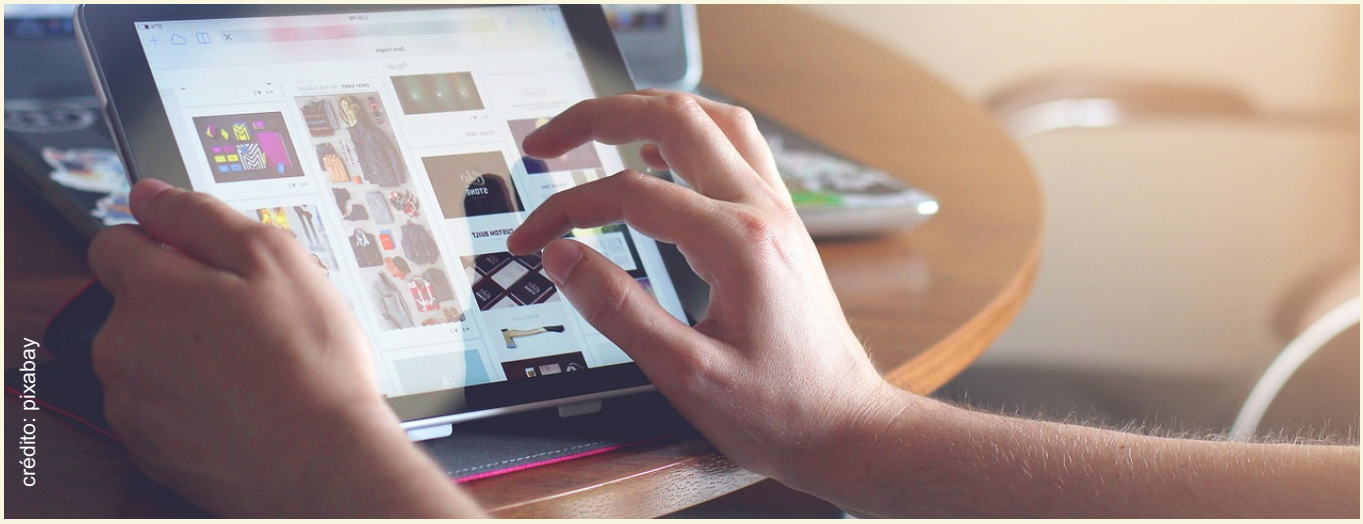
Muitos usuários pensam que suas máquinas não são interessantes para serem invadidas. Enganam-se porque é exatamente este tipo de máquina que os *hackers* querem invadir.

Por que uma máquina de um usuário não suspeito é fácil de ser invadida? O objetivo do invasor pode ser utilizar a máquina como um trampolim para invadir outras mais importantes, mascarando pistas sendo capaz de usar a máquina para realizar ataques distribuídos de negação de serviço (DDoS), por exemplo.

Podem também usar o computador do usuário para executar programas, alocar espaço no disco para disponibilizar programas piratas, vídeos, áudios ou arquivos com conteúdo pornográfico e além, buscar informações confidenciais, números de cartão de crédito ou registros de contas bancárias ou destruir dados por prazer, vaidade ou maldade.

O Windows oferece um *firewall* nativo normalmente habilitado na instalação. Existem disponíveis no mercado outros produtos mais sofisticados mas que requerem um conhecimento maior para configuração.

11 - Dispositivos móveis


crédito: pixabay

A questão de segurança em relação à mobilidade fica cada vez mais relevante devido à popularização de dispositivos como *smartfones* e *tablets*.

Atualmente, esses dispositivos sofreram grandes incrementos na sua capacidade de processamento e memória, além de apresentarem cada vez mais opções de conectividade.

Assim, eles se aproximam cada vez mais dos computadores pessoais. Não é surpresa que as ameaças existentes para *notebooks* e *laptops* de antes comecem a ser vistas proliferando em outros dispositivos móveis.

De fato, observa-se o surgimento de uma série de códigos maliciosos destinados a ataques a esses dispositivos. Esses ataques têm os objetivos mais diversos, como o roubo de informações, controle remoto e monitoração. Assim, muitas organizações começaram a perceber o risco dos dispositivos móveis.

Esses dispositivos tornaram-se parte do dia-a-dia das organizações da mesma forma que os *tablets* e *notebooks*.

Portanto, as organizações precisam começar a considerá-los como ferramentas de trabalho, sobre as quais deve existir uma gestão do ponto de vista de segurança.

Assim como nos computadores, nesse tipo de dispositivo, os cuidados devem ser os mesmos:

- Instalar aplicativos apenas de fontes confiáveis;
- Fazer *backup* de dados na nuvem ou no computador;
- Instalar e habilitar *software* antivírus

12 - Redes sociais

A utilização das redes sociais tornou-se imperiosa até mesmo para o trabalho.

Muitas comunicações importantes estão sendo feitas com várias plataformas (Facebook, Whatsapp, Instagram, etc.), principalmente com dispositivos móveis em função da correria do dia a dia e das facilidades e atrativos que elas proporcionam.

Por outro lado, as pessoas passaram a ficar mais expostas, já que tanto perfis pessoais quanto profissionais ficam acessíveis ao mundo da Internet.

Além disso, trafegam embutidos nessas mensagens todo tipo de *malwares* e *links* que podem remeter a *sites* falsos que podem comprometer a segurança do usuário das mais variadas formas.

***Fake-News*:** uma preocupação recente diz respeito à veiculação de notícias falsas e boatos que podem comprometer a imagem de pessoas e instituições e envolver o usuário em situações de desconforto e até mesmo penalidades civis. Veja mais informações no *link* abaixo: https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf

Seguem algumas dicas que podem ajudar o usuário a se prevenir de enrascadas, mas sempre o importante é o bom senso e a ética:

- Preservar a privacidade é uma regra básica de comportamento nas redes sociais, evitando expor o perfil indiscriminadamente, assim como o acesso indevido a informações pessoais e também profissionais;

- Ser criterioso ao aceitar convites para ingressar em grupos, comunidades e aceitar contatos;

- Utilizar o recurso de geolocalização com bastante cuidado, pois pessoas mal intencionadas podem estar monitorando deslocamentos indevidamente;

- Respeitar a privacidade dos outros, solicitando autorização para veicular imagens e notícias;

- Ser cuidadoso com arquivos anexados às mensagens, mesmo que sejam de pessoas conhecidas e

- Ter cautela na disseminação de notícias que podem ser falsas ("*fake news*"), caluniosas, geradoras de pânico ou simplesmente boataria.

13 - Resumidamente

Quais as precauções o usuário deve ter em relação à Segurança?

Computadores e Notebooks

- Usar antivírus e *firewall*;
- Atualizar o antivírus;
- Atualizar o sistema operacional;
- Não clicar em links recebidos por *e-mails* ou nas mensagens de redes sociais;
- Não executar arquivos recebidos por *e-mail* ou em mensagens de redes sociais;

Navegação

- Manter o navegador sempre atualizado;
- Não clicar em *links* suspeitos informando prêmios ou promoções;
- Só habilitar JavaScript, *cookies* e *pop-up* somente quando acessar *sites* confiáveis;
- Usar senhas complexas com letras, números e símbolos;

Celulares / dispositivos móveis

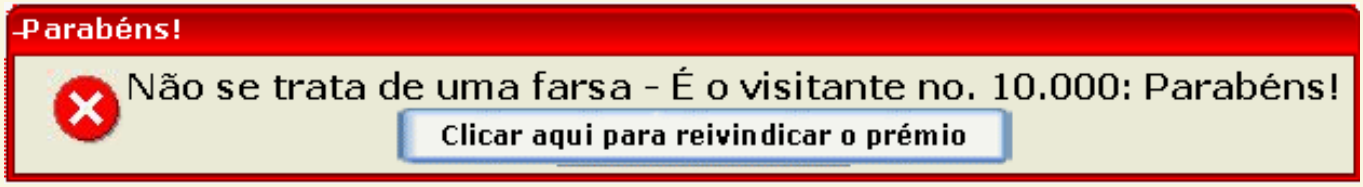
- Utilizar e atualizar o atívirus;
- Habilitar *bluetooth* só quando for utilizá-lo com outro dispositivo confiável;
- Fazer as atualizações no aparelho;
- Não aceitar e não executar qualquer arquivo enviado para o aparelho de origem duvidosa;

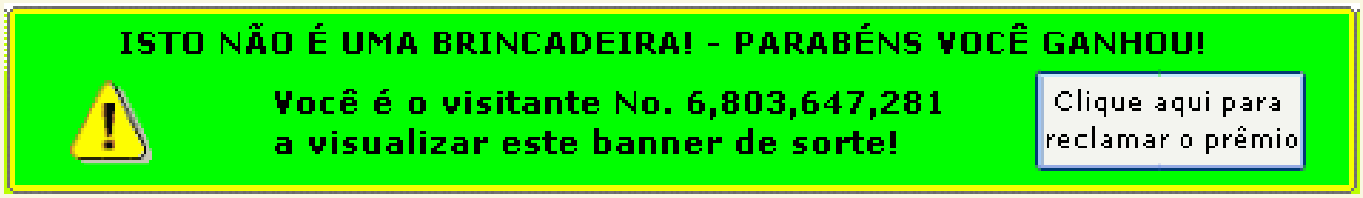
Redes sem fio

- Usar WEP ou WPA (acesso sem fio protegido) sempre que possível;
- Usar somente serviços com conexão segura;
- Não acessar aplicativos bancários em redes sem fio de bares, aeroportos, etc.

==========

Sempre desconfiar: a segurança e a tranquilidade dependem de nossas atitudes.





14 - Referências

- Cidale, Ricardo A. Vírus Digital: tudo o que as empresas precisam saber sobre a ameaça do vírus digital, como evitá-lo e como recuperar sistemas contaminados. McGraw Hill, 1990.
- Hatch James, Brian; Kurtz, George. Segurança Contra Hackers Linux. McGraw Hill, 2003.
- Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.
- Portal Terra, disponível em: <https://duvidas.terra.com.br/duvidas/600/quais-cuidados-devo-ter-para-minha-seguranca-na-internet/>.

CeTI-RP / STI