

Segurança na Informática

Prof. André Aparecido da Silva
Disponível em: www.oxnar.com.br/2bmas

Navegar é preciso...

Segurança
Digital

Navegar é
Preciso

Tipos de
Vírus

Tipos de
Vírus

Cuidados
na Internet



Tecnologia e Segurança

- Com o crescimento exponencial da internet e outras tecnologias de comunicação e interação cresce também os problemas derivados destas práticas. Isto deve – se a falta de informação por parte dos usuários, por sistemas sempre com alguma brecha de segurança ou por outros diversos motivos.



NAVEGAR É PRECISO

- A Internet já está presente no cotidiano de grande parte da população e, provavelmente para estas pessoas, seria muito difícil imaginar como seria a vida sem poder usufruir das diversas facilidades e oportunidades trazidas por esta tecnologia.



NAVEGAR É PRECISO

- Por meio da Internet você pode:
- Encontrar amigos;
- Fazer compras;
- Procurar melhores preços;
- Efetuar transações bancárias;
- Enviar declarações de Imposto de Renda, emitir boletos de ocorrências, agendar emissão de passaporte, consultar o acerto de museus, verificar programação de salas de cinemas e muito mais...

Tecnologia e Segurança

Estes são apenas alguns exemplos de como você pode utilizar a Internet para facilitar e melhorar sua vida.

Aproveitar esses benefícios de forma segura, entretanto, requer que alguns cuidados sejam tomados e, para isto, é importante que você esteja informado dos riscos aos quais está exposto para que possa tomar as medidas preventivas necessárias.

Alguns destes riscos são:

Acesso a conteúdos impróprios ou ofensivos:

Ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.



Xenofobia e Racismo



Páginas com opiniões

Mas lembre – se que estas paginas só existem porque tem muita gente que pensa igual a seus autores. Não é a toa que pessoas como Marcos Feliciano ou Pastores como Silas Malafaia fazem tanto sucesso nas redes sociais.



Páginas com opiniões

A internet em alguns pontos tem se tornado muito chata ao ponto de todos quererem impor a sua visão de mundo sem respeitar os outros.

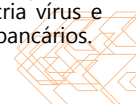
Como muitas vezes a TV também tenta impor suas visões de mundo.



Roubar dados Bancários

Uma das principais preocupações quando o assunto é segurança digital é o roubo de informações bancárias. Hackers podem aplicar golpes financeiros facilmente tendo o acesso ao seu computador.

E a situação piora quando estatísticas comprovam que o Brasil é um dos países que mais cria vírus e ameaças voltados para o roubo de dados bancários.



Como os golpes podem ser aplicados?

- A grande diferença do Brasil em relação aos outros países é que há um grande número de softwares personalizados voltados para o roubo de informações bancárias.

Enquanto hackers de outros países fazem uso de malwares mais genéricos, como o trojan Zeus, os hackers criam códigos específicos. Assim, surgiram vários métodos de captura de informações bancárias. Confira algumas delas:



O que são malwares?

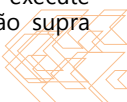
Termo proveniente do inglês "**malicious software**" ("**software** malicioso"); é um *software* destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).



Tipos de malware

Vírus de computador, *worms*, *trojans* (cavalos de troia) e *spywares* são considerados *malwares*.

Também pode ser considerada *malware* uma aplicação legal que, por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição supra citada.



Contato com pessoas mal-intencionadas

Existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e seqüestro.



Furto de Identidade

Assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.



Furto e perda de dados:

- Os dados presentes em seus equipamentos conectados a Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.



Invasão de privacidade

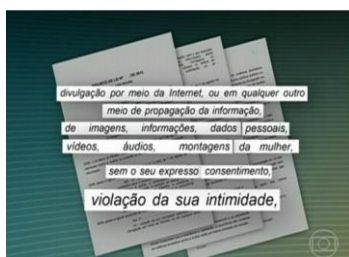
- A divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não sejam repassadas.



- Além disto, os sites costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.



Invasão de privacidade



Divulgação de boatos

- As informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo.
- Enquanto isto pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.



Dificuldade de exclusão:

- Aquilo que é divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado.



Dificuldade de exclusão:

- Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes.



Dificuldade de detectar e expressar sentimentos

- Quando você se comunica via Internet não há como observar as expressões faciais ou o tom da voz das outras pessoas, assim como elas não podem observar você (a não ser que vocês estejam utilizando webcams e microfones).
- Isto pode dificultar a percepção do risco, gerar mal-entendido e interpretação dúbia.



Dificuldade de manter sigilo

- No seu dia a dia é possível ter uma conversa confidencial com alguém e tomar cuidados para que ninguém mais tenha acesso ao que está sendo dito.
- Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.



Uso excessivo

- O uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.



Keyloggers

- Um keylogger é um programa que consegue enviar para o hacker todas as teclas que você digita em seu computador. Assim, a senha é descoberta facilmente. Atualmente, existem outros métodos que complementam o keylogger, permitindo o acesso a números de cartões de crédito e a senhas de redes sociais, e-mail, entre outros.



Keyloggers



Screenloggers

- O keylogger não é mais tão eficiente para o roubo de informações bancárias porque boa parte dos bancos criou sistemas em que, ao invés de digitar a senha, o usuário precisa clicar em botões específicos.



Screenloggers

- Em contrapartida, os hackers criaram um software que captura toda a tela ao redor do mouse, oferecendo acesso a todos os cliques feitos pelo usuário.



Screenloggers

- Novamente, os bancos agiram trocando os botões de posição ou deixando o botão apagado no momento em que é clicado. Os hackers criaram métodos para gravar em vídeo tudo o que o internauta faz e chegou-se à conclusão que a segurança feita pelos bancos ainda não era suficiente.



Tipos de Vírus de Computadores

- Worn (Verme eletrônico): Explora problemas nos sistemas computacionais.
- Bot: Controlado remotamente, bastante usado para tirar sites do ar. Não precisa da execução do arquivo para ser instalado.
- Trojan: O Cavalo de tróia recebido como um presente, proteção de tela, imagem pornográfica, após baixado



Tipos de Vírus de Computadores

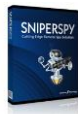
- Spam: Mensagem eletrônica recebida sem solicitação (propaganda).
- Spyware: É um software de monitoramento, pode ter usos legítimos, mas na maioria das vezes é instalado para fazer coisas ruins.



Software de Monitoramento

- Spybox: É um programa que monitora todas as ações do usuário.

É bastante comum para monitoramento de parceiros.



Plágio e violação de Direitos autorais

- A cópia, alteração ou distribuição não autorizada de conteúdo materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.



Como se prevenir?

- Atualize os sistemas:



Use UM bom anti-virus





Faça Backup



Use senhas boas

- No mínimo 8 caracteres;
- Mistura números e letras;
- Misture letras
- Não sejam dados conhecidos;
- Não use a mesma senha para tudo;
- Troque de senha regularmente;
- Associe a senha a algo fácil de lembrar



No celular

- Não deixe informações que demais pessoas não possam ver, afinal é fácil perder o celular;
- Use mecanismos de bloqueio para o celular;



No celular

- Faça uso de recursos remotos.
- Faça criptografia dos dados.
- Configure aplicativos de segurança do celular.



Engenharia social

- É a utilização de fatos que acontecem na própria sociedade para atacar. Por exemplo correspondência de um banco solicitando instalação de programas ou mensagem da receita federal ou ainda premio de um sorteio qualquer.



CSS3

- Fundo
 - Gradiente de cores no fundo
 - background: linear-gradient([[<angle> | to <side-or-corner>] ,]? <color-stop> [, <color-stop>]+;
 - <side-or-corner> = [left | right] || [top | bottom]
 - background: radial-gradient([[<shape> || <size>] [at <position>]? , | at <position> ,]? <color-stop> [, <color-stop>]+;



Demo 3 – JavaScript

Acessando serviços RESTful do lado do cliente



Padrões Web

