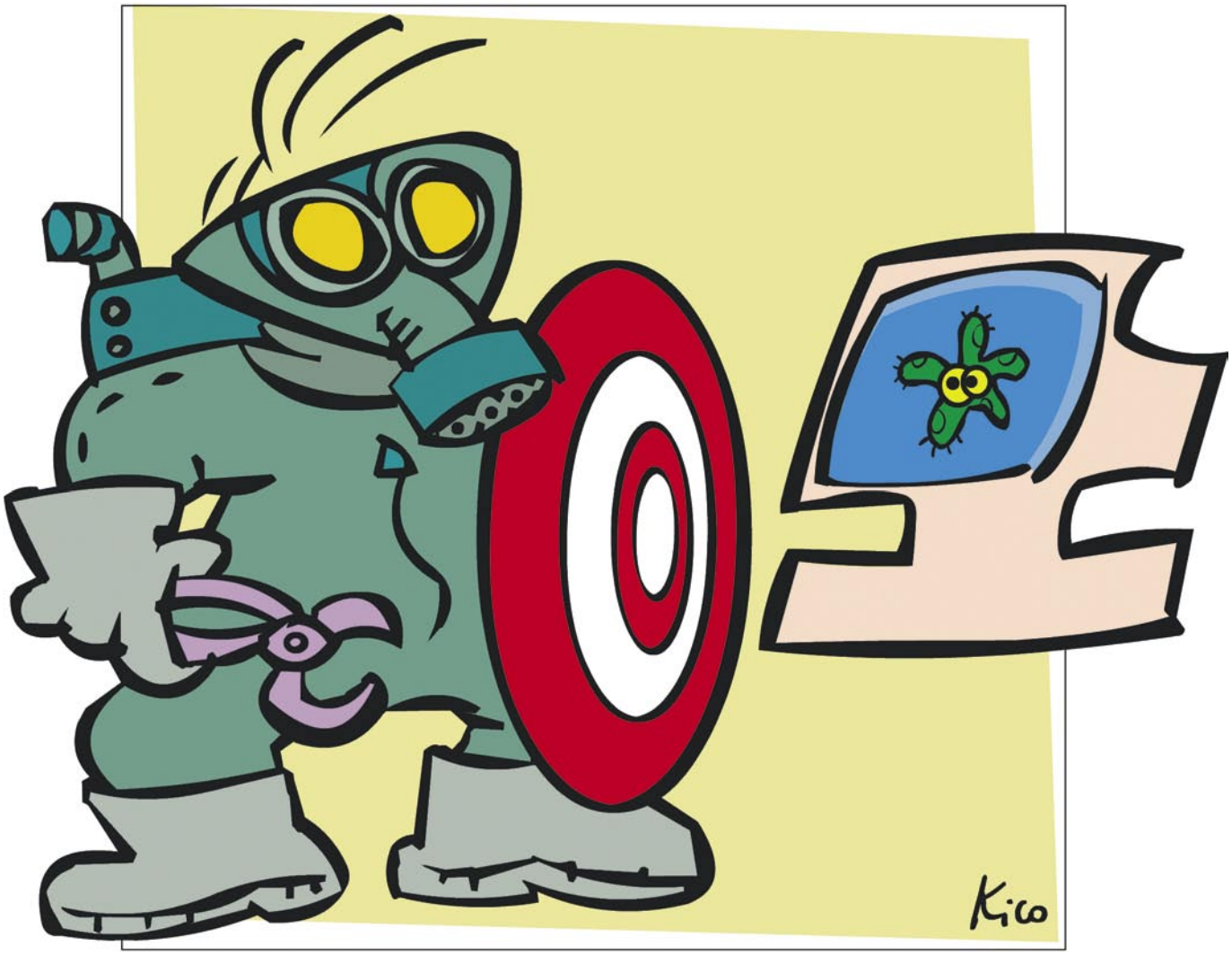
CADERNOS eletrônicos

Navegação segura

8



ESCOLA DO FUTURO
UNIVERSIDADE DE SÃO PAULO
acessa sp
PRODESP
Tecnologia da Informação
imprensaoficial
GOVERNO DO ESTADO
DE SÃO PAULO

Programa Acessa São Paulo

O Programa AcessaSP é uma iniciativa do Governo do Estado de São Paulo e tem como missão garantir o acesso democrático e gratuito às tecnologias de informação e comunicação, facilitando o uso dos serviços de governo e produção de conhecimento, promovendo os processos de participação pública e redes sociais para o desenvolvimento econômico, social, pessoal e da cidadania. Para cumpri-la, o Governo do Estado criou os Postos do AcessaSP, espaços com acesso gratuito à internet.

Para facilitar o uso dos equipamentos e atender a necessidades específicas, os usuários contam com monitores capacitados e comprometidos com o projeto para auxiliá-los. Esses monitores também são responsáveis pela gestão dos Postos.

Além disso, o Acessa São Paulo desenvolve uma série de atividades e projetos que amplificam e potencializam o impacto positivo que as tecnologias da informação e comunicação podem oferecer à população do Estado de São Paulo, tais como divulgação e facilitação do uso de serviços de governo eletrônico, produção de conteúdo digital e não-digital para a capacitação e informação da população atendida, promoção de ações presenciais e virtuais que possam contribuir para o uso cidadão da internet e das novas tecnologias, fomento a projetos comunitários com uso de tecnologia da informação, produção de pesquisas e informações sobre inclusão digital.

Outra preocupação do AcessaSP é trazer inovação para todas as atividades que executa e nos campos em que atua, em um processo de melhoria contínua que abrange desde a introdução de práticas de qualidade, elementos da cybercultura, da colaboração e da internet 2.0 até ações de intervenção social para a promoção do desenvolvimento e inclusão social. Com essa finalidade, desenvolvemos produtos como os MiniCursos Acessa, Dicionários de LIBRAS, a Rede de Projetos e a Capacitação de monitores e lideranças comunitárias.

As comunidades providas de um Posto são estimuladas a desenvolverem projetos e atividades que utilizem os recursos da tecnologia de forma criativa e educativa. Para isso, foi criado o portal na internet, para que os usuários dos Postos possam disponibilizar conteúdos elaborados pela comunidade e assim produzir conhecimentos próprios.

www.acessasp.sp.gov.br

Introdução

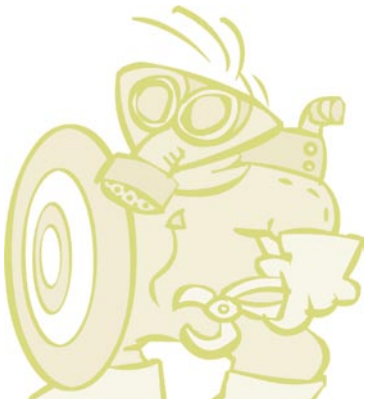
Descubra como dar maior segurança às suas informações, adotando práticas simples. Neste caderno você encontrará dicas de como proceder na Internet, como pensar em senhas mais seguras, quais práticas devem ser evitadas a fim de aumentar nossa privacidade e segurança on-line.

Conhecerá um pouco sobre os vírus, *spywares*, *trojans* (Cavalos de Tróia) e demais pragas que infestam a rede, disseminados por pessoas mal-intencionadas ou por seus próprios conhecidos, quando vítimas de *crackers*.

Aprenda também como identificar uma conexão segura e quais as características que esses sites devem ter para garantir que seus dados estejam protegidos.

Ao final, organizamos sugestões de remissão entre os Cadernos Eletrônicos mencionados, uma seção de links para downloads de programas freeware, tutoriais e dicas de segurança on-line, tudo para tornar sua navegação muito mais segura. Há também um glossário com os principais termos da informática e da Internet relacionados a esse tema.

Vamos começar?



Índice

1. Segurança virtual ameaçada? 5

2. Não seja uma “isca” 5

3. Como saber se a conexão é segura 7

4. Verificando os certificados dos sites 8

5. Etiqueta na rede é segurança 10

6. Vírus e outras pragas virtuais 10

7. Como impedir ataques 12

8. Segurança pessoal 12

9. Cuidado com as crianças 14

10. Como criar a senha ideal 15

Remissão entre cadernos e Links na Internet 15

Glossário 16

Acesse a versão on-line dos Cadernos Eletrônicos no link:
www.acessasp.sp.gov.br/cadernos

1 Segurança virtual ameaçada?

Provavelmente você já deve ter ouvido falar de vírus ou vermes de computador. Cavalo de Tróia e *spyware* também não devem ser palavras estranhas para você. Outros termos, porém, como *keyloggers*, não devem fazer parte do seu vocabulário. Entender um pouco sobre esse assunto fará com que se sinta mais seguro na web.

A Internet é uma nova maneira de estarmos no mundo e, assim como na vida real, o universo virtual exige medidas para preservarmos nossa segurança. Devemos ter na Internet o mesmo cuidado que temos de não fornecer informações pessoais para desconhecidos na rua ou de trancar a porta de casa antes de sair.

Na Web também há pessoas mal-intencionadas, conhecidas como *hackers* e *crackers*, que utilizam espiões (*spywares*) e vírus para invadir redes e máquinas com o objetivo de:

- Utilizar seu computador em alguma atividade ilícita, escondendo a real identidade e localização do invasor;
- Furtar números de cartões de crédito e senhas bancárias;
- Furtar dados do seu computador, como por exemplo, informações do seu Imposto de Renda;
- Utilizar a sua conexão para entrar na Internet como se fosse você;
- Atacar outros computadores através do seu;
- Destruir informações (vandalismo);
- Disseminar mensagens alarmantes e falsas (*spam*, correntes, etc);
- Ler e enviar e-mails em seu nome;
- Propagar vírus;
- Utilizar seu disco rígido como repositório de dados.

Por isso, todos os usuários de computador ou Internet estão sujeitos às diversas pragas virtuais. Mas calma! Não desista de navegar por causa disso. Já existem precauções que podem nos manter a salvo. Confira neste Caderno.

2 Não seja uma "isca"

Imagine a seguinte situação: você recebe uma mensagem por e-mail ou via serviço de troca instantânea de mensagens, em nome de um site de comércio eletrônico ou de uma instituição financeira (veja alguns exemplos na tabela a seguir). Muitas vezes, essas mensagens solicitam recadastramento ou confirmação dos dados do usuário para a participação em uma nova promoção, etc. Outras vezes, apenas abrem o computador para invasões. A mensagem, geralmente, tenta convencer o usuário a clicar em um link contido no texto ou em uma imagem. Esta prática é conhecida como *phishing* ou *phishing scam*.

Cartões virtuais que solicitam o clique em links, principalmente quando enviados por remetentes desconhecidos, podem ser uma artimanha para direcionar as pessoas a uma página de web falsificada.

A palavra *phishing* vem de uma analogia de *"fishing"* criada no sentido de "pescaria", em que "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

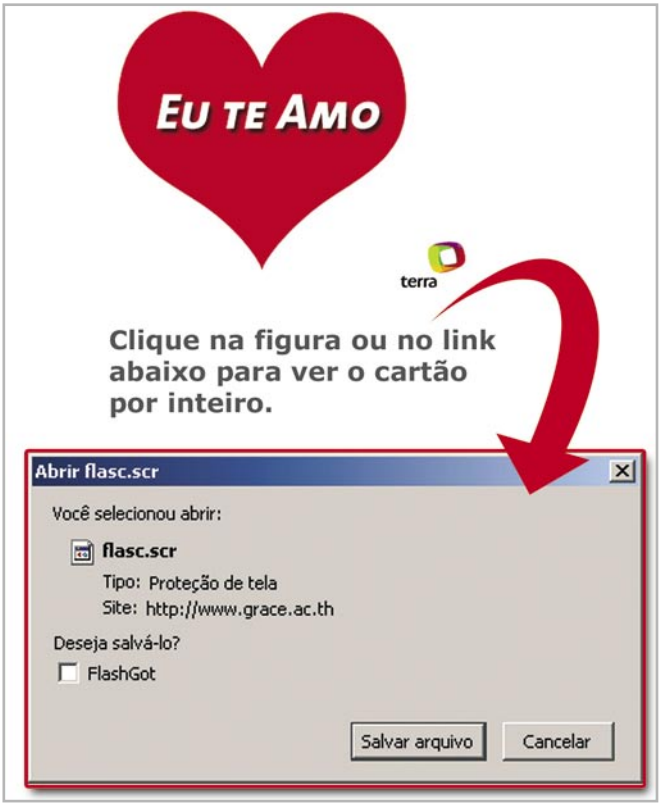
Como eles agem:

Os fraudadores utilizam técnicas para direcionar o leitor para uma página falsificada, apresentando o que parece ser um link verdadeiro relacionado à instituição mencionada na mensagem. Nesta página, serão solicitados dados pessoais como o número, data de expiração e código de segurança do seu cartão de crédito; ou os números da sua agência e conta bancária, dentre outros.

Ao preencher os campos disponíveis na página falsificada e clicar no botão de confirmação (em muitos casos o botão apresentará o texto "Confirmar", "OK", "Enviar", etc.), os dados serão remetidos para os fraudadores ou *hackers*.

A partir daí, eles poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros ou utilização dos mesmos para efetuar pagamentos, transferir valores para outras contas, etc.

Outra possibilidade é que, ao clicar no link do e-mail, os fraudadores tentem instalar arquivos espiões no computador.



Ao clicar no link sugerido, seu navegador pode abrir uma janela, solicitando que o arquivo seja "baixado" e instalado.

Cuidados:

Fique atento a algumas dicas para identificar este tipo de mensagem fraudulenta:

- Ao passar o cursor do mouse sobre o link, será possível ver o endereço da página na barra de status do programa leitor de e-mails ou navegador. Caso este link seja diferente do apresentado na mensagem, não deve ser acessado;
- Acesse a página da instituição que supostamente enviou a mensagem digitando o endereço diretamente na barra. Procure por informações relacionadas à mensagem que você recebeu;
- Sites de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados pessoais e financeiros de usuários são solicitados (mais informações no **capítulo 3** desse Caderno Eletrônico). Se a página não utilizar conexão segura, desconfie imediatamente;
- Em caso de desconfiança, se a página acessada apresentar página segura. leia o certificado do site (mais informações no **capítulo 4** deste Caderno). Caso o endereço mostrado no navegador seja diferente do apresentado no certificado, feche o browser imediatamente;
- Nunca aceite salvar ou instalar arquivos com extensão desconhecida (principalmente .exe), hospedados em páginas suspeitas. Só aceite downloads de programas quando feitos de páginas oficiais e certificadas.

Importante!

O remetente de uma mensagem ou e-mail nunca deve ser utilizado como parâmetro para garantir segurança, pois pode ser facilmente forjado pelos fraudadores. Há vírus que se auto-enviam para listas de endereço com o nome do proprietário, chegando para o destinatário com o nome de uma pessoa conhecida.

Exemplos de temas em mensagens de *phishing*:

Tema: Cartões virtuais
Mensagem: UOL, Voxcards, Humor Tadela, Terra, O Carteiro, Emotioncard, Criança Esperança.

Tema: SERASA e SPC
Mensagem: Débitos, restrições ou pendências financeiras.

Tema: Serviços de governo eletrônico
Mensagem: CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).

Tema: Álbuns de fotos
Mensagem: Pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.

Tema: Serviço de telefonia
Mensagem: Pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.

Tema: Antivírus
Mensagem: A melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.

Tema: Notícias/boatos
Mensagem: Fatos amplamente noticiados (ataques terroristas, tsunami, terremotos, etc), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).

Tema: Reality shows
Mensagem: BigBrother, Casa dos Artistas, etc -- fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.

Tema: Programas ou arquivos diversos
Mensagem: Novas versões de softwares, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.

Tema: Pedidos
Mensagem: Orçamento, cotação de preços, lista de produtos.

Tema: Discadores
Mensagem: Para conexão Internet gratuita, para acessar imagens ou vídeos restritos.

Tema: Sites de comércio eletrônico
Mensagem: Atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.

Tema: Convites
Mensagem: Convites para participação em sites de relacionamento (como o orkut) e outros serviços gratuitos.

Tema: Dinheiro fácil
Mensagem: Descubra como ganhar dinheiro na Internet.

Tema: Promoções
Mensagem: Diversos.

Tema: Prêmios
Mensagem: Loterias, instituições financeiras.

Tema: Propaganda
Mensagem: Produtos, cursos, treinamentos, concursos.

Tema: FEBRABAN
Mensagem: Cartilha de segurança, avisos de fraude.

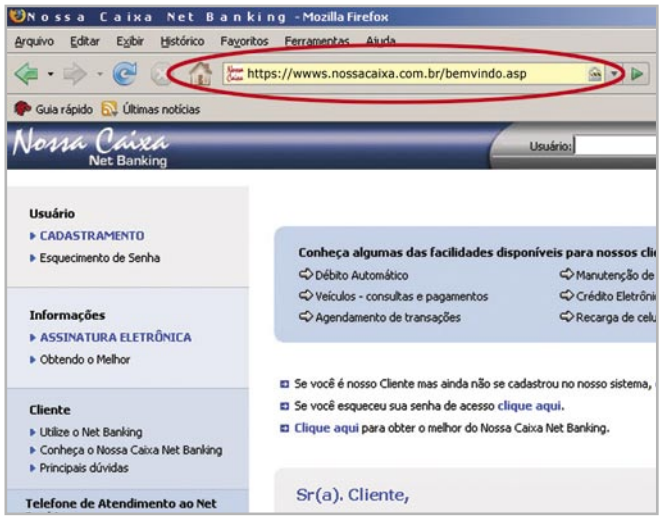
Tema: IBGE
Mensagem: Censo.

Cabe ressaltar que a lista de temas na tabela não é exaustiva, nem tampouco se aplica a todos os casos. Existem outros temas e novos temas podem surgir.

3 Como verificar se a conexão é segura

Existem pelo menos dois itens que podem ser visualizados na janela do seu browser e que significam que as informações transmitidas entre o navegador e o site visitado estão sendo criptografadas.

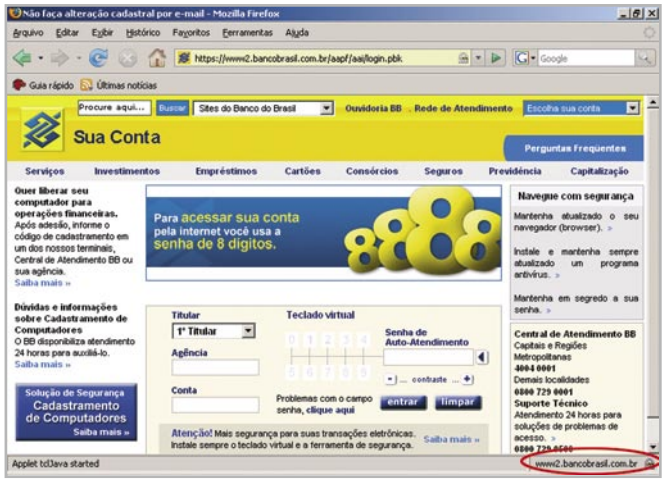
O primeiro está localizado onde a URL do site é digitado. O endereço eletrônico deve começar com “https://” (diferente do “http://” nas conexões normais). O “s” antes do sinal de dois pontos indica que o site possui conexão segura e, portanto, os dados serão criptografados antes de enviados.



Conexão segura no site Nossa Caixa, indicado pela sigla "https" no lugar do comum "http".

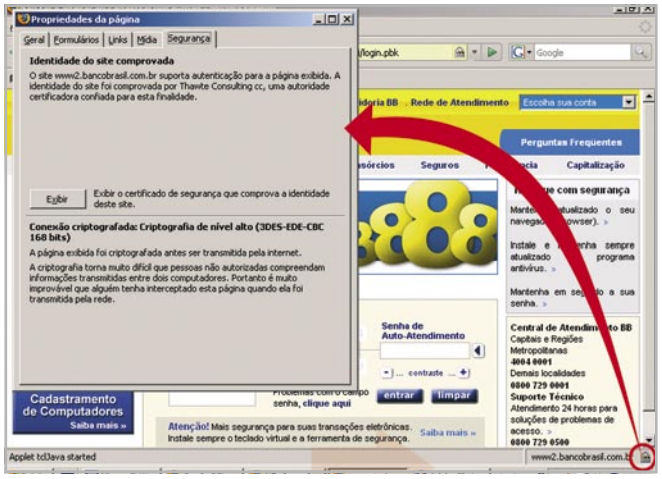
Alguns navegadores podem incluir outros sinais na barra de endereço do site, que indicandoconexão segura. No Firefox, por exemplo, esse campo muda de cor, ficando amarelo, e apresenta a imagem de um cadeado fechado do lado direito.

O segundo item a ser notado corresponde um desenho ou sinal, indicando que a conexão é confiável. Normalmente, o desenho mais adotado nos navegadores recentes é de um cadeado fechado na parte inferior direita do navegador (se o cadeado estiver aberto, a conexão não é segura).



No site do Banco do Brasil também contamos com a sigla "https" e o ícone do cadeado, indicando conexão segura.

Ao clicar sobre o cadeado, será exibida uma tela contendo as informações referentes ao certificado emitido para a instituição que mantém o site (trataremos disso mais adiante), bem como informações sobre o tamanho da chave utilizada para criptografar os dados.



Ao clicar sobre o cadeado, uma janela semelhante a essa se abrirá com todos os dados necessários para que você tenha certeza se a conexão é segura ou não.

Importante!

Verifique as informações do certificado clicando única e exclusivamente no cadeado exibido na barra de status do navegador. Fraudadores podem tentar forjar certificados, incluindo o desenho de um cadeado fechado no conteúdo da página.

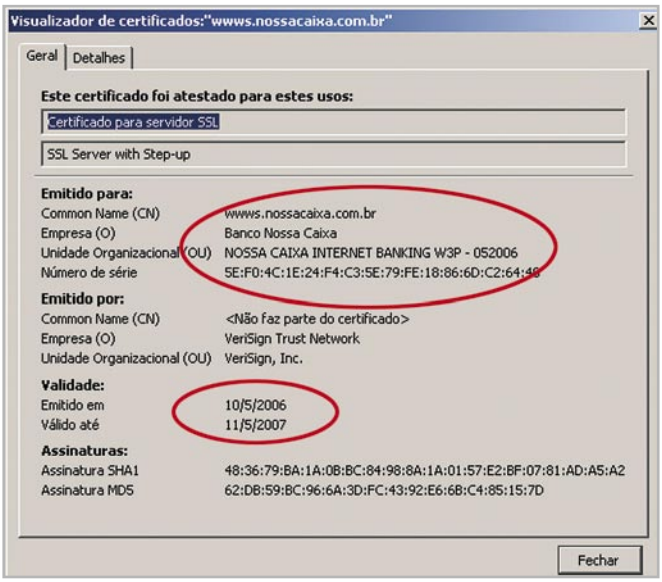
4 Verificando os certificados dos sites

Sempre que devemos comprovar nossa identidade mostramos o RG expedido por um órgão do Governo com autoridade para tal. Da mesma maneira, na Internet há empresas que certificam a identidade de portais ou sites, especialmente aqueles que solicitam dados confidenciais e pessoais dos usuários, como bancos, instituições públicas, etc.

Ao clicar no cadeado de uma página que tenha conexão segura, você terá acesso ao certificado que deve conter:

- O endereço do site;
- O nome da instituição (dona do certificado);
- O prazo de validade do certificado.

Ao entrar pela primeira vez em um site que usa conexão segura, seu navegador apresentará uma janela pedindo para confirmar o recebimento de um novo certificado. Então, verifique se os dados do certificado correspondem à instituição que você realmente deseja acessar e se seu navegador reconheceu a Autoridade Certificadora que emitiu o certificado.



Certificado do site Nossa Caixa.

Se, ao entrar em um site com conexão segura utilizado com freqüência, seu navegador apresentar uma janela pedindo para confirmar o recebimento de um novo certificado, fique atento. Uma situação possível é que a validade do certificado tenha vencido ou que o certificado tenha sido revogado por outros motivos e um outro tenha sido emitido em seu lugar. Mas isto também pode significar que você está recebendo um certificado ilegítimo e, portanto, está acessando um site falsificado.

Uma dica para reconhecer esta situação é que as informações contidas no certificado normalmente não corresponderão às da instituição que você realmente deseja acessar. Além disso, seu navegador possivelmente informará que a Autoridade Certificadora que emitiu o certificado não pôde ser reconhecida.

De qualquer modo, caso você tenha alguma dúvida ou desconfiança quanto aos certificados e às instituições que o emitiram, não envie informação para o site antes de entrar em contato com a empresa responsável para esclarecer o ocorrido.

Dicas resumidas:

1- Não digite nenhuma informação pessoal antes de certificar-se de que o site acessado possui conexão segura;

2- Utilize apenas uma janela do navegador: tente manter aberta apenas a janela que será utilizada na conexão, para não dispersar sua atenção;

3- Verifique a URL: na barra de endereços, deverá aparecer a sigla “https” no lugar de “http” das conexões normais;

4- Procure ícone do cadeado no canto inferior direito do seu navegador. Na imagem, o cadeado deve estar fechado para que a página tenha conexão segura;

5- Verifique o certificado: um duplo clique sobre o ícone do cadeado abrirá uma janela com os dados da empresa de segurança, emitido por entidade certificadora contratada pelo prestador do serviço.

6- Confira o endereço do certificado com o endereço da página: o certificado de segurança exibe o endereço verdadeiro que você deseja acessar. Ele deve ser idêntico ao da URL constante na barra de endereços do navegador;

7- Analise o conteúdo da página visitada: fique atento também aos dados solicitados. Nenhum banco ou administrador de cartão solicita na mesma página a sua senha de acesso via Internet, o número de cartão de banco ou de crédito, a senha do banco e outros códigos de segurança;

8- Caso você perceba, seguindo os passos acima, que a sua conexão não é segura, feche o navegador imediatamente para interromper a conexão.

É bom saber

Sites de compras on-line, como Submarino.com, Americanas.com, ou qualquer outro que comercialize produtos pela Internet, devem conter as mesmas características mencionadas para os sites bancários.

Sempre que seus dados pessoais ou financeiros forem solicitados, verifique a segurança da sua conexão.

5 Etiqueta na rede é segurança

Os riscos de cair nas armadilhas dos *hackers* não estão apenas em abrir e-mails suspeitos ou rodar no computador CD's que contenham programas alterados. Acessar sites pouco confiáveis ou misturar atividades pessoais com as profissionais são dois exemplos de como a falta de etiqueta na hora de navegar na Internet pode causar dor de cabeça.

Muitos usuários, acreditando que não estavam fazendo nada de errado quando baixaram uma música, por exemplo, podem fazer com que a empresa onde trabalham seja processada por permitir que seus funcionários baixem livremente arquivos protegidos por leis de direitos autorais.

Outro perigo é que não há qualquer garantia contra contaminação dos arquivos baixados.

Os softwares legais são uma garantia de não conter programas maliciosos, além de oferecer o suporte técnico da empresa desenvolvedora, dentre outras vantagens.

Dica

Procure não misturar assuntos pessoais com profissionais. Ao manipular mensagens relacionadas à empresa em casa ou em ambientes públicos, como cyber cafés - por não oferecerem a mesma infra-estrutura de segurança de um ambiente corporativo - as informações valiosas podem ser interceptadas por terceiros para serem usadas mais tarde para chantagens, por exemplo.

6 Vírus e outras pragas virtuais

Já vimos que no *phishing* o usuário é convencido a clicar em um link e fornecer seus dados em sites falsos. Mas e as pragas que se instalam no seu computador sem você saber?

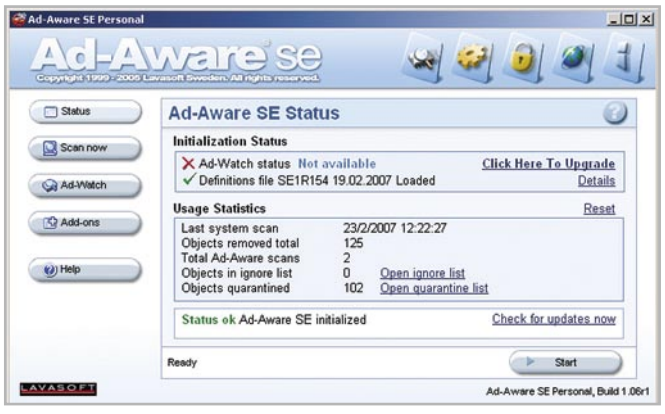
O *spyware,* ou espião, recebe este nome justamente porque tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Como os espiões de filmes, ele pode utilizar as informações coletadas para o bem ou para o mal.

Algumas empresas utilizam o serviço de *spyware* para monitorar os gostos das pessoas que freqüentam seu site e assim colocar os destaques da página de acordo com informações que mais as atraiam.

Os *hackers* instalam o *spyware* para monitorar todos os acessos a sites enquanto o usuário navega na Internet e assim conseguir dados sigilisos relevantes.

Sempre que o usuário acessa determinados sites de bancos ou de comércio eletrônico, o *keylogger* ou *screenlogger* é ativado para a captura de senhas bancárias ou números de cartões de crédito (consulte o **Glossário** ao final desta edição para saber mais).

Mas já existem programas para encontrá-los e destruí-los, como por exemplo, os anti-*spywares* "Spybot – Search & Destroy" e o "Ad-aware", ambos *softwares* gratuitos.



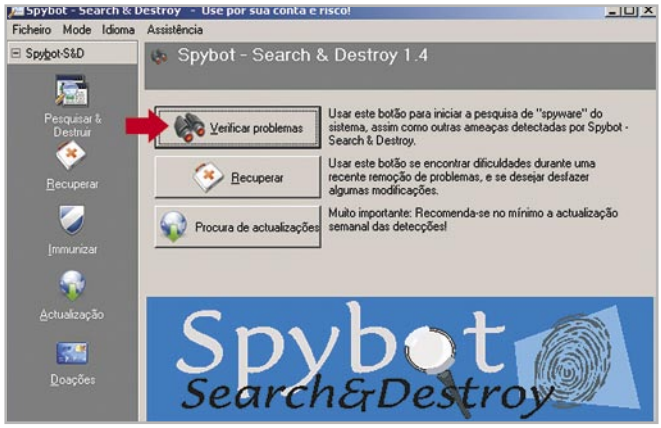
Tela inicial do Ad-Aware, anti-*spyware* **gratuito.**

Na maior parte dos casos, o usuário dá abertura ao espião quando acessa sites pouco confiáveis, especialmente pornográficos e com *pop-ups* (aquelas janelinhas que pulam na sua tela com propagandas).

Importante!

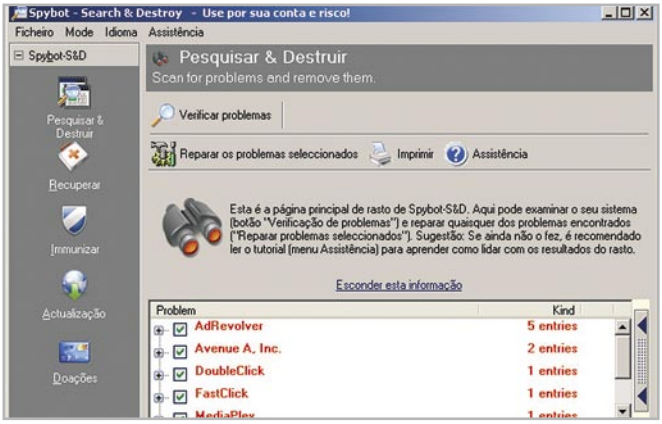
Antes de verificar possíveis spys e vírus no computador, certifique-se de que seu anti-vírus ou anti-spyware está atualizado.

Um anti-*spyware* é um software de segurança que tem o objetivo de detectar e remover *adwares* e *spywares*, os programas espiões que monitoram a atividade dos usuários no momento em que conectam a Internet.



Tela inicial do "Spybot": boa opção para eliminar spys.

Muitos antivírus já incorporam detecção de *spyware* e *adware*, mas um anti-*spyware* específico ainda faz parte da programação de segurança da maioria dos usuários, porque possui um banco de dados mais atualizado e específico, que possibilita a busca e localização precisa desse tipo de arquivo.



Spybot em funcionamento: vários arquivos identificados como possíveis "espiões".

Os vírus são outra praga da Internet. O nome não é por acaso; eles agem como seres vivos que se autocopiam e multiplicam dentro de um computador "hospedeiro" muito rapidamente. Na primeira oportunidade, transmitem-se para computadores vizinhos e muitas vezes causam danos letais, sendo necessária a limpeza total da máquina para instalar todos os programas novamente.

Você pode pegar vírus abrindo arquivos ou ao instalar programas de procedência duvidosa e desconhecida, obtidos pela Internet, em pen drives, CDs, DVDs, etc.

Felizmente, existem os antivírus, como o "Avast!", que são gratuitos e muito eficientes para detectar e destruir essas pragas. Consulte a seção "Links na Internet" para ver os sites que oferecem esses programas.

O Avast! é apenas uma das opções de antivírus gratuitos disponíveis na Internet.

Um antivírus é um software responsável pela detecção, desinfecção e remoção de pragas digitais como vírus, *trojans* (cavalos de tróia), *worms* e qualquer outro tipo de código malicioso, não se limitando somente aos vírus como o nome sugere. Alguns antivírus também removem *adwares* e *spywares*, tarefa antes reservada apenas aos anti-*spywares*.

O antivírus funciona com um banco de dados chamado de lista de definição, que contém informações para que o antivírus consiga identificar quais arquivos são benéficos (parte dos programas e sistemas que temos instalados) e quais são maliciosos (foram instalados nos computadores sem autorização).

O AVG é um dos mais tradicionais anti-vírus gratuitos. A nova versão está em Inglês.

O que isso significa? Em outras palavras quer dizer que, para que o antivírus consiga detectar um, é necessário que ele esteja na lista de definição. Esse é o motivo pelo qual os antivírus requerem atualização constante: para manter a lista sempre renovada e, assim, poder detectar os problemas mais recentes.

É bom saber

Nos postos do Acessa São Paulo a utilização do Linux foi também uma opção de segurança, pois podemos dizer que praticamente não existem vírus nem spywares para este sistema.

7 Como impedir ataques

Com o grande fluxo de informações que circulam pela rede, foi necessário estabelecer uma maneira de não "misturar as estações".

Por isso, a estrutura da Internet utiliza portas para comunicação entre as máquinas. As portas funcionam como guichês de atendimento das antigas repartições públicas, em que cada um trata de um assunto específico. Por exemplo, para acessar programas de webmails seu navegador acessa a porta 110, para conversar em chats a porta é a 6687.

Para nossa segurança, devemos trancar as portas de casa para que estranhos não entrem, assim também é com o computador: devemos usar um *firewall* para trancar as portas que não estão sendo usadas a fim de impedirmos a invasão de *hackers* e *crackers*. Estes costumam entrar pela "porta dos fundos" ou *backdoor*.

Por isso, muitas empresas bloqueiam as portas com números acima de 1024 que são referentes a vários aplicativos de entretenimento, como salas de bate-papo, vídeo-conferência, jogos on-line e softwares de relacionamento.

É bom saber

Todo cuidado é pouco. Um firewall bem configurado deixa deixa aberta apenas as portas estritamente necessárias aos aplicativos que o usuário utiliza, navegação, e-mail e entretenimento, se o ambiente for doméstico. No ambiente de trabalho restrições são ainda mais severas.

8 Segurança pessoal

Além das armadilhas para capturar dados na Internet, há cuidados que devemos tomar para não expor a nossa vida pessoal.

Ao utilizar softwares sociais, como Orkut e MySpace, suas mensagens (ou *scraps*) podem ser lidos por qualquer um. Por isso, são muito utilizados por pessoas mal-intencionadas para conhecer hábitos, gostos, informações pessoais a fim de coagir, chantagear e até seqüestrar pessoas.

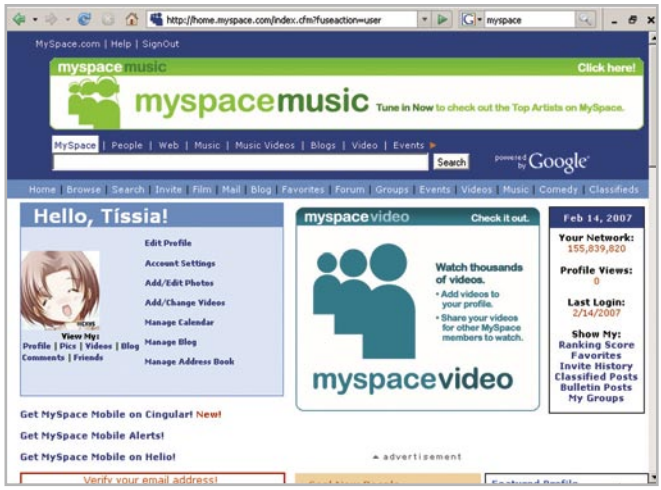
Especificamente sobre o Orkut, a Ponline 2006, aponta que apenas 20,6% dos usuários acredita que esse tipo de software social serve para "acompanhar os passos da vida alheia" e 20,1% para "Expor sua vida pessoal".

Para conhecer a Ponline, acesse: www.acessasp.sp.gov.br/ponline/

Podemos ver um exemplo de uma mensagem em que o usuário do Orkut divulgou os dados do local onde trabalha e qual cargo exerce. Práticas como essa devem ser evitadas.

Algumas dicas são importantes para evitarmos ameaças virtuais:

- Não mande recados com dados pessoais como números de telefone, documentos, endereços residenciais e informações sobre seus familiares e amigos (como árvores genealógicas, datas de aniversário, etc.), dentre outros;
- Procure não marcar encontros por meio de recados (como aniversário de fulano, no bar tal, na data tal, às X horas), nem dar informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, etc.);
- A participação de um usuário em determinados tipos de comunidades também pode fornecer muita informação para terceiros. Por exemplo, a comunidade de donos de um determinado veículo, ou dos freqüentadores do estabelecimento X, pode dizer qual é a classe social de um usuário, que locais ele gosta de freqüentar, etc;
- Limite o acesso aos seus dados pessoais para apenas as pessoas de interesse, pois todas as informações poderão ser vistas por qualquer pessoa.



Tela inicial do software social Myspace: é necessário proteger seus dados pessoais.

Além dos cuidados acima, ao escrever em seu blog vale ficar atento para não citar informações, tais como:

- Dados sobre o seu computador (dizendo, por exemplo, "...comprei um computador da marca X e instalei o sistema operacional Y..."");
- Dados sobre os softwares que utiliza (por exemplo: "...instalei o programa Z, que acabei de obter do site W...").

Dica

É importante avaliar com cuidado quais informações você disponibilizará nos sites softwares sociais, principalmente aquelas que poderão ser vistas por todos, e de que comunidades você participará. Estas informações podem não apenas ser utilizadas por alguém mal-intencionado (por exemplo, em um ataque de engenharia social), mas também para atentar contra a segurança física do próprio usuário.

Exemplo de perfil retirado do software social Orkut: quanto menor o número de informações pessoais, tanto melhor!

9 Cuidado com as crianças

Nos dias de hoje, a facilidade de aprender informática disponibiliza para as crianças e adolescentes uma gama de conteúdos ilimitada de informações, entretenimento, diversão, mas também de pornografia e violência. E é aí que pode estar o perigo. Por isso, os pais e responsáveis precisam ter um cuidado especial.

Novos tempos exigem novas medidas: além da segurança física, agora os pais devem se preocupar com a segurança virtual.

Há no mercado diversos softwares que bloqueiam o acesso a determinados sites e até programam o tempo de acesso e o horário. Mas a solução mais eficiente para esse impasse ainda é o bom e velho diálogo. Se você deseja se informar antes da conversa, há muitos sites que trazem cartilhas para ajudá-lo.

Dentre os perigos a que os pequenos estão expostos, a pedofilia tem sido o mais grave crime on-line. Os criminosos se passam por crianças para enganá-las, freqüentam salas de bate-papo, fazem perfis falsos em sites de redes sociais e assim conseguem informação pessoais das crianças e até marcam encontros.

Página inicial de Navegação Segura do AcessaSP.

Dica

O Portal do AcessaSP conta com uma nova página, dedicada especialmente à navegação segura. Lá, você poderá encontrar reportagens, sites com conteúdos especializados, links de denúncia, dentre outros.

Deve ficar claro que a violência sexual pode vir, ou não, acompanhada de violência física. Sendo assim, expor a criança a cenas de sexo via Internet ou intimidá-la para praticar o ato sexual via computador, sejam com palavras ou em frente a uma webcam, é considerado uma violência porque parte-se do princípio de que uma criança ou adolescente ainda não tem maturidade bio-psico-sexual para consentir este tipo de atividade sexual. Não é à toa que o Código Penal Brasileiro considera crime sexual toda e qualquer relação de caráter sexual com pessoas menores de 14 anos.

Página inicial do Safernet: um dos maiores sites de denúncias de crimes na internet.

Dica

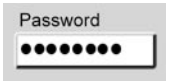
Denuncie crimes virtuais! Links Safernet é um dos maiores sites de denúncias de crimes na Internet. Outros links como esse podem ser encontrados na página de Navegação Segura do AcessaSP.

Para combater esse tipo de crime, dentre outros tantos cometidos pela internet (como roubo de dados pessoais, senhas e assédio moral), a justiça conta também com a atuação dos próprios internautas para denunciar sites, conteúdos e perfis de usuários que pratiquem ou estimulem esses crimes.

Existem hoje vários endereços eletrônicos e organizações que combatem crimes virtuais. Nesses links, o usuário pode, muitas vezes, fazer denúncias.

Mantenha-se informado, leia reportagens, dicas e conheça links sobre segurança na Internet acessando a página de Navegação Segura do AcessaSP no endereço:
http://www.acessasp.sp.gov.br/html/modules/news2/index.php .

10 Como criar a senha ideal



As senhas (*password*) são quase tão antigas quanto a humanidade. Destinadas a privilegiar pessoas que detinham acesso a palácios, passagens secretas, ou qualquer outro tipo de edificação, elas têm a característica principal de ser um código que somente o seu detentor tem conhecimento.

Os sistemas de informação de hoje em dia têm vários métodos de conceder acesso, que vão dos mais antigos, como o reconhecimento das impressões digitais tal qual o utilizado em nossa carteira de identidade, aos ultramodernos, como o mapeamento eletrônico da íris.

Mas no abracadabra cibernético, a boa e velha senha ainda domina o mercado das fechaduras eletrônicas. Por isso, é imprescindível que uma série de cuidados sejam tomados, de modo a evitar que outras pessoas deduzam nosso código mágico e entrem em domínios que deveriam ser exclusivamente nossos. Veja algumas dicas:

1- Tenha pelo menos três senhas divididas em “grupos”: lazer, trabalho e banco;

2- Troque-as mensalmente;

3- Crie senhas longas;

4- Varie ao máximo o tipo de caractere: use símbolos, letras e números;

5- Quando só puder usar números, faça combinações pouco prováveis e sem seqüência;

6- Não escolha palavras existentes em dicionários - piratas virtuais usam softwares específicos para adivinhá-las;

7- Se quiser usar palavras, escreva-as de forma errada (substitua a letra “a” por “@”, por exemplo);

8- Nunca anote suas senhas, e só as compartilhe quando extremamente necessário (caso de marido e esposa, por exemplo).

Remissão entre os Cadernos Eletrônicos

Caderno 1: ***Como usar e gerenciar seus e-mails.***
Caderno 4: ***Navegação e pesquisa na internet.***
Caderno 5: ***Publicação de conteúdo na Internet***

Links na Internet

Downloads:

www.baixaki.ig.com.br - *Baixaki, vários antivírus e antispyawares gratuitos;*

http://superdownloads.uol.com.br/windows/index.html - *Superdownloads, diversos antivírus e antispywares free;*

www.grisoft.com - *AVG, antivírus Free 7.1;*

http://www.avast.com/eng/download-avast-home.html - *Avast, antivírus gratuito;*

http://www.lavasoftusa.com/ - *Ad-Aware, antispyware gratuito;*

http://www.spybot.info/pt/tutorial/index.html - *Spybot, antispyware gratuito;*

Dicas de segurança, tutoriais e informações:

http://www.acessasp.sp.gov.br/html/modules/news2/index.php - *Navegação Segura do AcessaSP: dicas, reportagens e links sobre segurança na Internet;*

http://www.condeca.sp.gov.br/index.asp - *Conselho Estadual dos Direitos da Criança e do Adolescente;*

http://cartilha.cert.br/ - *Cartilha sobre segurança na Internet;*

http://www.antispam.br/ - *Cartilha sobre Spans e como evitá-los);*

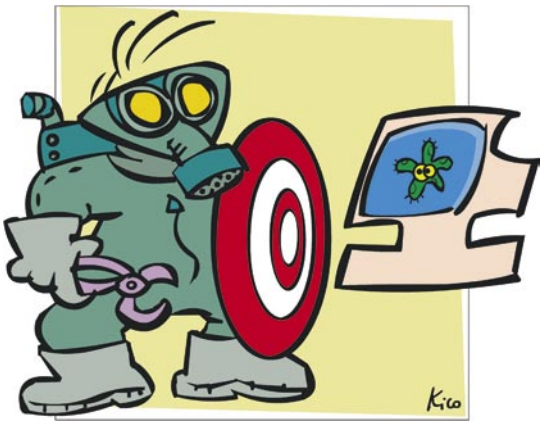
www.hackerteen.com.br - *HackerTeen;*

http://www.hackerteen.com.br/pdf/cartilha.pdf - *Dicas de segurança dos filhos para pais.*

http://www.acessasp.sp.gov.br/ponline/ - *Pesquisa on-line anual realizada pelo AcessaSP. Veja as respostas no site.*

Glossário

Adware: programa que vem oculto a um outro, baixado da Internet, sem que o usuário tenha conhecimento. Uma vez instalado, sempre que o computador estiver conectado à rede, passa a exibir anúncios interativos, o que torna o sistema mais lento.
Backdoor: em português, "porta dos fundos". Termo utilizado para definir portas abertas em um sistema, que não são documentadas e permitem acesso de terceiros sem que sejam notados. Podem ser criadas tanto pelo responsável pelo sistema (como meio de acesso emergencial) como também por pessoas interessadas em invadir o sistema e roubar informações.
Backup: cópia de segurança das informações, utilizada em caso de perda de dados.
Cracker: indivíduo que possui conhecimentos avançados de informática, mas, ao contrário dos *Hackers*, utiliza esses conhecimentos para destruir sistemas e ficheiros alheios, sem se preocupar com os resultados dos seus atos.
Criptografia: ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.
Download: em inglês "load" significa carga e "down" para baixo. Fazer um download significa baixar um arquivo de um servidor, descarregando-o para o nosso computador.
EXE: programa executável. De um modo geral, todos os programas .exe são suspeitos, a menos que a sua procedência seja bem conhecida.
Firewall: aparelho ou software responsável por isolar segmentos de rede, podendo fechar seletivamente portas de comunicação e implementar uma série de regras.
Freeware: qualquer software (programa) oferecido gratuitamente na rede ou nas publicações especializadas em suportes como CD-ROM.
FTP: File Transfer Protocol ou protocolo de transferência de arquivos. É uma maneira de copiar arquivos via Internet. Os arquivos são disponibilizados e localizados em servidores ou em computadores pessoais por um programa servidor de FTP.
Hacker: termo originário do inglês, usado para designar um especialista em Informática. Um hacker é, pela definição correta um "Problem Solver" - aquele que resolve problemas.
Http: Acrossemia de "Hyper Text Transfer Protocol" ou "Protocolo de Transferência de Hipertexto". É o protocolo que permite o funcionamento da interface gráfica da Internet.
Internet: rede mundial de computadores. Trata-se de uma rede planetária de computadores que cooperam entre si.
Keylogger: programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
Link: ligação, elo, vínculo. Nas páginas da web é um endereço que aparece sublinhado, ou em uma cor diferente da cor do restante do texto. Um link nada mais é que uma referência cruzada, um apontador de um lugar para outro na web. Assim, eles permitem um vínculo com uma imagem, um arquivo da mesma página ou de outras da web, a partir de um clique do mouse.
Macros: pequenos programas que têm por finalidade automatizar tarefas como impressão, mala direta etc.
Navegador: navegador, programa para abrir e exibir as páginas da Web como o Explorer, da Microsoft, o Navigator, da Netscape etc.
Cavalo de tróia: programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. Na maioria das vezes se comporta como vírus.
Phishing scam: a palavra phishing (de "fishing") vem de uma analogia criada pelos fraudadores, onde "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.
Ponline: pesquisa on-line anual realizada pelo AcessaSP para dar contorno ao perfil de usuário do Acessa e seus hábitos na Internet.
Pop-ups: janela que surge separadamente quando navegamos em um determinado site, geralmente para apresentar um anúncio.
Posto do AcessaSP: ponto de acesso público à Internet construído pelo Governo do Estado de São Paulo.
Protocolo: é um conjunto de regras que os computadores usam para se comunicar e, a partir dessa comunicação, produzir algum resultado útil como a navegação em sites, a transmissão de e-mail ou o download de arquivos.
Screenlogger: forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado. Veja também Keylogger.
Servidor: computador que está do outro lado da conexão. No caso de uma conexão web, por exemplo, o servidor remoto é um servidor web da empresa.
Site: palavra inglesa que significa lugar. O site é o lugar no qual as páginas da web podem ser encontradas.
Softwares Sociais: ambientes ou softwares que englobam um conjunto de ferramentas de comunicação que facilitam e estimulam a interação entre seus usuários, principalmente no sentido de formarem redes de relacionamento. Essas ferramentas englobam correio eletrônico (e-mail), comunicadores instantâneos, fóruns, grupos de notícias, assim como qualquer outro tipo de comunidade virtual.
Spywares: códigos maliciosos que se instalam na sua máquina geralmente por meio de janelas do tipo pop-up e que visam registrar hábitos de navegação – assim como as senhas que porventura forem digitadas – para depois enviar tudo ao hacker que os desenvolveu.
URL: Universal Resource Locator (URL) é o endereço de um recurso ou ficheiro disponível na Internet, ou seja, o código para localização universal que permite identificar e acessar um serviço na Web.
Vermes ou worms: se diferem dos vírus por se espalharem de forma automática e rápida. Além de não dependerem de uma intervenção direta do usuário para se tornarem ativos, eles se reproduzem automaticamente de um sistema para outro, criando cópias a partir deles mesmos na máquina da vítima. Sua maior complexidade os faz maiores em tamanho (Kbytes); daí o nome de vermes.



Defenda-se

Quando a Internet foi criada, nos anos de 1960, seu uso era restrito aos meios acadêmicos. Essa característica permitia que as relações estabelecidas na rede fossem parecidas com as de uma cidadezinha no interior do país: a confiança mútua era grande, todos eram bem-vindos ao pequeno mundo digital.

Assim, as questões relacionadas à segurança eram secundárias, pois os pesquisadores, além de se conhecerem, desejavam trocar seus dados e suas descobertas.

Na década de 1990, as coisas mudaram drasticamente. Houve a entrada massiva dos computadores domésticos, em conjunto com os servidores comerciais, que mudaram a cara da rede. Surgia uma Internet adulta, multifacetada, composta de grandes grupos comerciais, consumidores, profissionais liberais, adolescentes, pais, mães, e toda a sorte de pessoas que, definitivamente, pensam de maneira bem diferente dos primeiros internautas.

Hoje desejamos privacidade e necessitamos manter nossos dados pessoais, exames médicos, saldo bancário, nossos documentos digitais, nossas correspondências e outras informações e dados confidenciais fora do alcance de pessoas mal-intencionadas que também fazem parte da rede. Os mecanismos de proteção digital disponíveis são os mais variados possíveis para nos oferecer segurança de navegação.

Neste caderno vamos aprender um pouco mais sobre segurança no mundo digital para que você possa ter acesso a todos os benefícios da Internet sem correr riscos desnecessários e indesejáveis.

www.acessasp.sp.gov.br

GOVERNO DO ESTADO DE SÃO PAULO

Governador — Cláudio Lembo
Secretaria de Estado da Casa Civil — Rubens Lara

IMPRENSA OFICIAL DO ESTADO DE SÃO PAULO

Diretor-Presidente — Hubert Alquéres
Chefe de Gabinete — Émerson Bento Pereira

Rua da Mooca, 1921, Mooca
CEP 03103-902 São Paulo/SP
Tel.: Grande SP (11) 6099-9725
Demais localidades 0800-123-401
sac@imprensaoficial.com.br
www.imprensaoficial.com.br

PROGRAMA ACESSA SÃO PAULO

Coordenadores — Maria Amélia K. Fernandes
Ricardo Kobashi

Rua da Mooca, 1921, Mooca
CEP 03103-902 São Paulo/SP
Tel.: (11) 6099-9579 / 6099-9641
e-mail: acessa@sp.gov.br
www.acessasp.sp.gov.br
www.cadernos.futuro.usp.br

ESCOLA DO FUTURO - USP

Reitora — Suely Vilela
Vice-Reitor — Franco Maria Lajolo
Pró-Reitora de Pesquisa — Mayana Zatz
Supervisão Científica — Brasilina Passarelli
Coordenação Editorial e Pedagógica — Drica Guzzi, Hernani Dimantas e Carlos Seabra
Coordenação de Produção — Drica Guzzi e Tíssia Nunes
Roteiro, Pesquisa e Redação — Tíssia Nunes
Paula Buratini
Maria da Conceição C. Oliveira
Projeto Gráfico/DTP — Ronald Chira e Ludimyla Russo
Web Designer — Araciara Teixeira
Ilustração da Capa — Francisco Sá Godinho (Kiko)
Revisão — Marina Iemini Atoji e Mariane Suwa
Colaborador — Júlio Boaro

Av. Profº. Lucio Martins Rodrigues, Trav. 4 - Bloco 18
CEP 05508-900 São Paulo/SP
Tel.: (11) 3091-6366 / 3091-9107
www.futuro.usp.br
www.lidec.futuro.usp.br

Os Cadernos Eletrônicos foram desenvolvidos pelo Laboratório de Inclusão Digital e Educação Comunitária da Escola do Futuro da USP (LIDEC) para o Programa Acessa São Paulo do Governo do Estado de São Paulo, por meio de sua Secretaria da Casa Civil. A reprodução parcial ou integral deste caderno é permitida e estimulada somente para fins não comerciais e mediante citação da fonte. Dezembro/2006.

Cadernos Eletrônicos **1**

Como usar e gerenciar seus e-mails

Cadernos Eletrônicos **6**

Uso da impressora e tratamento de imagens

Cadernos Eletrônicos **2**

Editoração e processamento de textos

Cadernos Eletrônicos **7**

Comunidades virtuais - listas, chats e outros

Cadernos Eletrônicos **3**

Planilha eletrônica e gráficos

Cadernos Eletrônicos **8**

Navegação Segura

Cadernos Eletrônicos **4**

Navegação e pesquisa na Internet

Cadernos Eletrônicos **9**

Multimídia: vídeo e áudio no computador

Cadernos Eletrônicos **5**

Publicação de conteúdo na Internet

Cadernos Eletrônicos **10**

Web 2.0 e aplicativos on-line