

MIÚDOS NA WEB.

UMA BRINCADEIRA DE CRIANÇAS?



PANDA
SECURITY

One step ahead.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



O volume de novo malware (vírus, spyware e outros códigos maliciosos) que surgiu em 2007 aumentou dez vezes comparativamente ao ano anterior. Além do mais, os ciber-criminosos descobriram novas ferramentas como o instant messaging (programas como o MSN Messenger ou o Yahoo! Messenger, etc.), os programas de partilha de ficheiros (como o eMule ou o Kazaa) e os blogs, utilizando-os como novas formas de infectar os utilizadores e roubar-lhes informação confidencial.

Por outras palavras, os riscos da Internet estão a aumentar e as crianças, por estarem menos informadas, são também as mais vulneráveis.

Abaixo, explicamos algumas das principais ameaças da Internet a que as crianças estão expostas, e as melhores formas de as proteger. Muito do ónus da protecção recai sobre os pais e educadores, que devem controlar o que as crianças fazem na Internet, instruindo-as sobre como desfrutar das novas tecnologias de uma forma segura e responsável.

Dados significativos: As crianças e a Internet



Segundo dados da Save the Children, mais de 13 milhões de crianças na Europa possuem acesso frequente à Net. A maioria acede à Web pela primeira vez antes dos 10 anos de idade.

Segundo um estudo realizado em 2004 pela Kleiner and Lewis, 90 por cento das crianças nos EUA entre os seis e os dez anos de idade acedem regularmente à Internet. Em 2006, um estudo da American Psychological Association (APA) coloca o número de crianças que navegam regularmente na Web, entram em chatrooms ou utilizam o IM, entre os 75 e 90 por cento.

Dados compilados na EU relatam uma história similar. O Euro-barómetro revela que 64 por cento das crianças na Dinamarca, Holanda e no Reino Unido são utilizadores da Internet; na Suécia verifica-se 63 por cento, na Finlândia 62 e na Estónia 60 por cento. Com a excepção da Grécia (15%), do Chipre (20%) e da Eslováquia (30%), os dados são bastante semelhantes no resto da Europa. Um estudo de Outubro de 2008, patrocinado pela Entidade Reguladora das Telecomunicações (ERC) sobre a recepção dos meios de comunicação faz algumas revelações preocupantes sobre a utilização da Internet pelos jovens em Portugal. Por exemplo, a maioria das crianças utiliza o computador para conversar on-line, descarregar músicas ou trocar informações, muitas sem o conhecimento dos pais, e a maioria de forma completamente autónoma.

Em termos absolutos, e segundo dados da Save the Children, mais de 13 milhões de crianças na Europa possuem acesso frequente à Net: quatro milhões têm menos de 12 anos de idade e nove milhões encontram-se os 12 e os 17 anos. O Reino Unido encontra-se no topo do ranking dos países cujas crianças utilizam a Internet. Relativamente aos riscos, cerca de 49 por cento das crianças entrevistadas pela Save the Children afirmam ter encontrado na Internet conteúdos que as assustaram ou preocuparam.

Resumindo, a Internet faz parte das vidas diárias das crianças. Elas despendem várias horas ligadas à Net, seja na escola ou em casa.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



Principais riscos

As crianças e jovens estão expostos a uma série de riscos na Internet, desde a infecção dos computadores por malware a pessoas com identidades falsas a influenciá-los para um encontro pessoal.

Neste documento veremos uma listagem das principais ameaças e como os pais e crianças as podem combater.



As ferramentas de instant messaging utilizam endereços de e-mail e passwords para identificar os utilizadores. Isto dificulta saber quem se encontra no outro lado.

Instant messaging e e-mail

O instant messaging (através de programas como o MSN Messenger, o Yahoo! Messenger, o Google Talk, etc.) tornou-se num canal de comunicação bastante difundido entre crianças. Este fenómeno não passou despercebido aos ciber-criminosos, o que aproveitaram rapidamente como o principal canal para as suas actividades.

Uma das ameaças mais perigosas para as crianças e jovens que utilizam estas ferramentas são as falsas identidades (alguém a fazer-se passar por outra pessoa para enganar potenciais vítimas). Nestes programas os utilizadores são autenticados através de um endereço de e-mail e de uma password. Logo, se alguém aceder à conta de um contacto, nada avisará o utilizador que a pessoa com quem está a conversar não é quem diz ser. Se possui ficheiros partilhados com esse contacto, o atacante conseguirá aceder-lhes livremente. É por isso que se torna importante não partilhar qualquer informação confidencial (dados pessoais, moradas, números de identificação, dados bancários, etc.) através de canais inseguros como o instant messaging.

Um perigo ainda mais sinistro relativamente à falsificação de identidade é a sua utilização por pedófilos. A sua estratégia é ganhar a confiança dos jovens e marcar um encontro em pessoa, ou persuadi-los a enviarem fotografias comprometedoras. Fazem passar-se por outros jovens, fotógrafos profissionais e muitas outras falsas identidades.

A educação é sem dúvida a melhor forma de proteger os jovens desta particular ameaça. Conselhos como "não falar com estranhos" são tão válidos no contexto online como na vida real, e as crianças devem ter confiança suficiente para falarem abertamente com os pais ou educadores em caso de dúvidas.

Outro potencial risco do instant messaging é a infecção por vírus ou códigos maliciosos. Quase 60 por cento dos worms (códigos maliciosos que se propagam pelos próprios meios) detectados pelo PandaLabs nos primeiros seis meses do ano foram desenvolvidos para se propagarem através de aplicações de instant messaging. Alguns foram desenvolvidos para capturar passwords para bancos online. O risco no caso de infecção afecta obviamente os pais para além das crianças, já que serão os seus dados bancários e consequentemente o seu dinheiro que estará em jogo.

Existem medidas simples que podem ser tomadas para impedir que estes códigos maliciosos alcancem os computadores através de instant messaging: Não executar qualquer ficheiro nem clicar em nenhum link que receba por este canal. Pelo menos não sem antes verificar se a pessoa que o enviou é realmente quem afirma ser.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



O melhor conselho contra o malware distribuído através de aplicações de mensagens é não executar qualquer ficheiro nem clicar em nenhum link recebido através deste canal.

O e-mail é outra fonte de risco para os jovens. Neste caso existem diversas ameaças:

- Em primeiro lugar temos o spam. Este tipo de correio indesejado é frequentemente utilizado para promover tudo, desde casinos online a fármacos. As crianças são muito mais susceptíveis de acreditarem nas mensagens que estes e-mails contêm, com todos os riscos associados. Podem aceder a casinos online e tornarem-se viciadas em jogo, ou podem adquirir fármacos ou mesmo drogas com sérios riscos para a saúde.
- A seguir, temos as falsas ofertas de emprego. Apesar de não representar uma ameaça séria para os mais jovens, pode representar um perigo para adolescentes. Estas mensagens normalmente contêm ofertas de trabalho fantásticas. Prometem grandes salários em troca de muito pouco ou nenhum esforço. Tudo o que é necessário é o número de uma conta bancária para onde o dinheiro será enviado, e então, em troca de uma comissão, o receptor deve reenviar o dinheiro para outra conta. Parece demasiado bom para ser verdade, e qualquer adulto suspeitará. No entanto, um jovem à procura de dinheiro fácil poderá cair nesta armadilha. Tornar-se-á cúmplice de um crime, já que o objectivo destas transferências é a lavagem de dinheiro proveniente de actividades criminosas.
- Outro risco é a entrada de vírus e malware nos computadores. Os códigos maliciosos distribuídos através destas mensagens destinam-se a enganar os utilizadores levando-os a clicar num link ou a transferir um ficheiro (que causa a infecção) utilizando uma série de assuntos atractivos: filmes, fotografias eróticas, transferência de jogos, etc. Esta técnica é conhecida como engenharia social. Muitos adultos são enganados por estas técnicas, logo é fácil verificar como as crianças podem cair na armadilha.

A melhor forma de proteger os jovens contra estas ameaças é encorajá-los a suspeitar de e-mails de fontes desconhecidas. Devem estar conscientes de que muito do que é escrito nestas mensagens é falso e que nunca debes executar ficheiros nem clicar em links neste tipo de e-mails.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



Os riscos de programas de partilha de ficheiros

A partilha de ficheiros através de redes P2P é outra grande fonte de infecções. Muitos códigos maliciosos – normalmente worms – são copiados para pastas destes programas com nomes atractivos (nomes de filmes, programas, etc.) na tentativa de encorajar outros utilizadores a transferirem os ficheiros e a executá-los nos seus computadores.

Isto é, para todos os propósitos, outra variante da engenharia social: os nomes dos ficheiros podem ser deliberadamente destinados a crianças ou jovens, que sem o saberem estarão a permitir a entrada de software malicioso nos seus computadores.

É por isto que as crianças devem saber que ficheiros podem transferir e quais os que devem evitar. É também uma boa ideia analisar qualquer ficheiro com uma solução de segurança antes de o abrir pela primeira vez. Se surgir uma mensagem de erro ou uma janela a solicitar a transferência de uma licença ou de um codec deverá suspeitar, já que o ficheiro deverá conter um vírus ou outro malware.

Muitos códigos maliciosos copiam-se para as páginas Web mais visitadas, com o objectivo de serem transferidas e executados pelos utilizadores.

Redes sociais e blogs

Os sites de redes sociais (como o MySpace ou o Facebook) são muito utilizados para partilha de fotografias e vídeos, para encontros e conversas, etc, tal como os blogs. Um componente comum destas páginas é a necessidade de criar um perfil pessoal para lhes aceder. Estes perfis contêm frequentemente dados como nome, idade, etc.

As crianças devem ser recordadas que em geral não é necessário fornecer este tipo de informações, e que um endereço de e-mail e um nome (que poderá ser falso) são suficientes. Não deverão fornecer dados como a idade, morada, e em particular, fotografias deles próprios.

Muitos jovens utilizam blogs como uma espécie de diários pessoais. Como tal, estes jornais online contêm frequentemente muito mais informação do que é aconselhável. É particularmente importante evitar a publicação de dados que possam identificar o utilizador como menor, ou que possa revelar a morada, local onde estuda, etc.

Em determinadas redes sociais, como o MySpace, é possível partilhar ficheiros com outros utilizadores. As crianças devem prestar particular atenção para o que partilham e a quem fornecem permissão para aceder a esta informação. Não existe problema em publicar, por exemplo, fotografias, desde que estejam protegidas com password apenas distribuída por amigos e família.

Os pais devem conhecer estes novos serviços, como funcionam e quais os riscos existentes. Devem também instruir as crianças a utilizarem estas ferramentas de forma segura e correcta.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



As funcionalidades dos smartphones, como o Bluetooth e o acesso à Internet, estão a tornar os telemóveis vulneráveis a ataques.

Telemóveis com Internet: um novo risco

Segundo um relatório da Frost & Sullivan, o aumento da sofisticação dos telemóveis irá torná-los num dos principais alvos dos cibercriminosos nos próximos anos. O estudo defende que tecnologias como o Bluetooth (que permite a partilha sem fios, de ficheiros entre dispositivos) e o acesso à Internet de alta velocidade estão a tornar estes dispositivos vulneráveis a ataques.

Os telemóveis são muito utilizados por crianças e adolescentes. Os riscos que enfrentam são assim semelhantes aos comentados acima relativamente aos PCs.

Primeiro os serviços de instant messaging para dispositivos móveis já estão difundidos. As crianças podem entrar em chatrooms a partir de qualquer lugar, e os riscos são os mesmos que detalhamos anteriormente: roubo de identidade, predadores, infecções de malware, etc.

O spam está a começar a atingir os telemóveis. Mensagens SMS a promover todo o tipo de produtos e serviços já existem há alguns anos. Muitos destes anúncios estão relacionados com pornografia. Isto significa que não é só através dos seus computadores que as crianças estão expostas a este tipo de conteúdos, mas também nos seus telemóveis.

Os pais devem por isso controlar o que as crianças fazem com os seus telemóveis. Para tal, é aconselhável fornecer aos mais novos telemóveis que não incluam funções que possam representar uma fonte de risco, e no caso das crianças mais velhas, aconselhe-as sobre como devem utilizar o seu telefone. Recorde-as que não devem atender chamadas de fontes duvidosas nem marcar encontros com estranhos.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



O risco de infecção

Vimos anteriormente as diferentes formas como os utilizadores podem infectar os seus computadores (links em e-mails ou por instant messaging, downloads de redes de partilha de ficheiros infectados...). Existem inúmeros perigos em ter códigos maliciosos em execução no sistema.

Primeiro, tal como mencionado acima, se as crianças partilharem um computador com os seus pais, existe o risco de infectar o PC com um Trojan bancário ou outro malware semelhante que possa roubar dados bancários quando os adultos utilizam o computador.

Mas o malware não é apenas uma ameaça para os adultos. Também representa riscos para as próprias crianças. Por exemplo, é muito fácil ser afectado por adware. Este tipo de código malicioso é utilizado para mostrar banners, pop-ups e outros anúncios em computadores infectados. Para os adultos, isto poderá ser mais incómodo do que outra coisa (no entanto é preciso cuidado, já que alguns transferem Trojans para os sistemas infectados), mas o risco é maior para as crianças e jovens, dado que alguns anúncios promovem ligações para páginas Web com conteúdos pornográficos. Por isso as crianças podem encontrar pornografia nos seus próprios PCs, sem sequer terem visitado páginas com estes conteúdos.



Se os mais novos partilharem o computador com os pais, existe o risco de uma utilização menos cuidadosa poder infectar o computador.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



Conselhos práticos para pais

- 1 Fale com os seus filhos:** O primeiro passo para proteger os seus filhos é falar com eles. Deverá conhecer as páginas que visitam, com quem falam, o que gostam de ver, etc. Não os deixaria sair de casa sem saber para onde vão e com quem vão, logo, não deverá deixá-los aceder à Internet sem saber o que estão a fazer.
- 2 Aprenda por si, e passe o conhecimento para os seus filhos:** Para muitos pais a Internet ainda é um mundo desconhecido. Alguns utilizam-na para procurar informação, ler o jornal ou transferir músicas, files e outros ficheiros, mas muitos outros, os serviços e as páginas que os seus filhos utilizam são completamente desconhecidos. Como tal é muito importante conhecer as ferramentas que a Internet oferece às crianças, e quais os riscos que existem e como evitá-los. Quando obtiver estes conhecimentos já pode aconselhar os seus filhos sobre como utilizarem a Internet de forma segura.
- 3 Defina regras firmes para a utilização da Internet:** Deve estabelecer regras claras e firmes, controlando o tempo máximo online e a forma como utilizam a Internet. Certifique-se que cumprem as regras, especialmente no que diz respeito à utilização da Web de noite. Outro aspecto a considerar é a localização dos computadores em casa: se possui apenas um PC para toda a família, deve encontrar-se numa divisão familiar e não no quarto da criança.
- 4 Proíba as crianças de fornecerem informação confidencial:** Deve instruir os seus filhos para não fornecerem dados como o nome, morada e fotografias pela Internet. Aconselhe-os a utilizar nomes falsos ou pseudónimos em fóruns e mostre-lhes como criar palavras-passe seguras (misturando letras maiúsculas com minúsculas) para impedir que ciber-criminosos ou outros utilizadores maliciosos acessem às suas contas de e-mail ou messaging.
- 5 Ensine os seus filhos a estarem atentos às aparências:** As aparências também iludem na Internet. Já verificámos códigos maliciosos disfarçados de codecs ou trailers de filmes; as formas como os pedófilos se fazem passar por outras pessoas para estabelecer contacto com crianças, ou a forma como mensagens que parecem provir de um contacto conhecido podem estar infectadas. Logo, na Web as coisas nem sempre são o que parecem. Ensine os seus filhos a estarem alerta e para não fazerem nada que possa colocar em causa a sua segurança ou privacidade.
- 6 Instale uma solução de segurança eficaz:** Para proteger os seus filhos de códigos maliciosos, a melhor estratégia é possuir uma solução de segurança eficaz e actualizada. A Panda oferece soluções para utilizadores domésticos que não se limitam a eliminar malware, bloqueando também páginas Web que possam infectar os computadores, filtrando spam e, no caso do Internet Security, inclui uma funcionalidade de controlo parental que lhe permite seleccionar que páginas os seus filhos poderão aceder.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



Conselhos práticos para crianças

- 1 Não cliques em links:** Quando conversas por instant messaging ou recebes um e-mail, nunca cliques directamente em quaisquer links. Se a mensagem ou e-mail vierem directamente de alguém que conheces, então escreve o endereço no browser. Se não conheceres a pessoa que enviou, o melhor é ignorá-la.
- 2 Não transfiras ficheiros de fontes duvidosas:** Certamente recebes com frequência mensagens instantâneas convidando-te a descarregar uma fotografia, uma música ou um vídeo. Por vezes, este ficheiro pode não ter sido enviado pela pessoa cujo nome aparece como remetente, mas sim por um programa malicioso que infectou o teu computador e que se está a distribuir para outros utilizadores. Como salvaguarda, o melhor a fazer é perguntares ao teu contacto se realmente te enviou algo. Caso não o tenha enviado, informa-o que possivelmente foi infectado para que possa eliminar o ficheiro e alertar os seus contactos.
- 3 Não fales com estranhos:** Em chatrooms ou em instant messaging, nunca podes saber com certeza com quem estás a falar. Especialmente em comunidades online, onde algumas pessoas nunca se encontraram na vida real. Nunca deves criar amizades com estranhos, e em nenhuma circunstância deves encontrar-te com eles na vida real.
- 4 Não forneças informação confidencial pela Internet:** Nunca envies informação privada (os teus dados, a tua morada, etc.) por e-mail ou instant messaging, e nunca publiques este tipo de informação em blogs ou fóruns. Deves também ter cuidado quando crias perfis para serviços como o FaceBook ou Myspace. Nunca deves incluir informação confidencial como a tua idade ou morada. É aconselhável não utilizares o teu nome verdadeiro, mas sim um nome falso ou um pseudónimo.
- 5 Fica atento a qualquer suspeita:** Se um programa que não te recordas de ter instalado começar a mostrar falsas infecções ou pop-ups a convidar-te para comprar um produto, tem cuidado. Podes ter algum tipo de malware instalado no teu computador.
- 6 Não executes ficheiros suspeitos:** Se a tua solução de segurança te informar que um ficheiro pode conter ou contém malware, não o abras. Apaga-o apenas.
- 7 Fala com os teus pais ou professores:** Se tens alguma questão acerca disto, se encontrares algo suspeito ou receberes e-mails ofensivos ou perigosos, fala com um adulto. Eles serão capazes de te aconselhar.



MIÚDOS NA WEB. UMA BRINCADEIRA DE CRIANÇAS?



Conselhos práticos para professores

Os professores têm um papel importante no fornecimento da informação sobre as formas correctas de utilizar as novas tecnologias, a crianças e jovens acima de tudo, já que os computadores são actualmente comuns nas salas de aula. É por isso que fornecemos uma série de recomendações a seguir:

- 1 Descubra:** Procure e leia informação acerca das ameaças da Internet. Descubra o que são e quais as suas consequências, e como pode transmitir esta informação aos jovens.
- 2 Desenvolva um plano de educação relacionado com segurança das TI:** Tal como os jovens aprendem a lidar com computadores e com a Internet, devem também aprender sobre os potenciais perigos. Desta forma, garantirá que se mantêm seguros desde o primeiro momento. O melhor procedimento é desenvolver um plano a seguir, preparar o que lhes transmitirá e fornecer a documentação que julgue necessária.
- 3 Torne as suas explicações agradáveis e práticas:** uma boa forma de ensinar estes conceitos é utilizando exemplos práticos. Pode demonstrar alguns dos perigos da Internet mostrando aos seus alunos alguns dos efeitos que podem causar. Descubra novas histórias relacionadas com casos reais.
- 4 Ensine-os a proteger-se:** Durante aulas práticas, mostre aos jovens como configurar um antivírus e criar palavras-passe seguras, e explique como comprar online de forma segura, etc

