



NAVEGAÇÃO NA INTERNET

Nuno Martins

Índice Geral

[História da Internet alguns dados relevantes 1](#_Toc509405226)

[Segurança da Internet no Computador 1](#_Toc509405227)

[CYBERBULLYING 2](#_Toc509405228)

[Redes Sociais 2](#_Toc509405229)

[SPAM 3](#_Toc509405230)

[Phishing 3](#_Toc509405231)

[Segurança da Internet no Telemóvel 3](#_Toc509405232)

[Segurança nas consolas de jogos 4](#_Toc509405233)

[Riscos associados à Internet 5](#_Toc509405234)

[Perigos e Fraudes na Internet 5](#_Toc509405235)

[e-Drugs 6](#_Toc509405236)

[A Dependência da Internet e os Efeitos na Saúde 7](#_Toc509405237)

[Sintomas 7](#_Toc509405238)

Índice de figuras

[Figura 1 - E-Drugs 7](#_Toc509386090)

História da Internet alguns dados relevantes

A Internet nasceu como um projeto alternativo e não como uma prioridade entre os académicos e investigadores. É o resultado da interação entre a ciência, a pesquisa básica universitária, os programas de investigação militar nos Estados Unidos da América e a contracultura radical. Esta poderosa tetralogia chama a atenção, pois representa um momento histórico de convergência entre os agentes que desenvolvem alguma simpatia pela inovação de sistemas informáticos, mas que não se encontram formalmente envolvidos, pelo menos não como parte 235 de um processo de investigação institucionalizada. Por outras palavras, a explicação do nascimento da Internet não pode ser classificada como um projeto claro e preciso, em que as partes envolvidas partilharam um ideal comum a perseguir. Pelo contrário, assemelha-se mais a uma tarefa lúdica de comunicação que se desenvolve nos tempos livres ou como uma forma de descanso intelectual do trabalho científico complexo; para outros era mais uma das mais diversas formas de interpretação que poderiam ser consideradas para a explicação e divulgação do processo de transmissão de dados.

A Internet pode ser considerada como muito mais do que simples tecnologia. É um meio de comunicação, interação e organização de tonalidades democráticas cujo controlo social não tende a ser feito por alguns e a sua utilização não é considerada um meio para obtenção de benefícios económicos cativos para grupos de utilizadores. Embora esta questão seja discutível, pode-se tentar seguir os caminhos que sustentam tal afirmação. Por um lado, considera-se que o verdadeiro negócio para as empresas são os artefactos tecnológicos, tais como computadores, servidores e todos os acessórios que são necessários tanto de hardware como de software, tornando-se cada vez mais evidente que alguns fabricantes têm encontrado o seu nicho de oportunidades no desenvolvimento tecnológico de artefactos cada vez mais rápidos, mais pequenos, com melhor desempenho e maior versatilidade e, não menos importante, o baixo preço para o consumidor. (Correia, 2011)

Segurança da Internet no Computador

À medida que aumenta o uso da Internet pelas crianças e adolescentes, também aumentam as preocupações sobre sua segurança on-line. Proporcionar um ambiente seguro requer uma compreensão profunda dos tipos de riscos on-line que os jovens usuários da Internet enfrentam, bem como das soluções mais eficazes para a mitigação desses riscos. Apesar da quantidade bastante significativa de pesquisas conduzidas com relação a esses riscos, aprimorar a segurança de crianças/jovens na Internet permanece um desafio. Em parte, isso se dá uma vez que as definições dos termos e categorias relevantes para a segurança on-line (tais como “cyberbullying”) frequentemente variam, o que torna imprecisa a comparação das estatísticas e constatações entre as fontes. Além disso, há sobreposições complexas entre os diferentes subtópicos de segurança on-line. No geral, esses fatores podem dificultar a identificação de lacunas específicas nas pesquisas e conhecimento existentes. Se essas lacunas puderem ser melhor identificadas e supridas, uma compreensão baseada nos dados sobre os problemas que os jovens enfrentam poderia desempenhar um papel fundamental no direcionamento das decisões de política com relação à segurança on-line. Para abordar essa questão, o presente estudo visa apresentar:

1). Uma visão geral da pesquisa sobre segurança on-line existente envolvendo uma ampla gama de categorias.

2). Uma análise das principais constatações.

3). Uma identificação das lacunas no conhecimento.

4). Um conjunto de recomendações para pesquisa em áreas específicas que seja capaz de promover o diálogo sobre políticas relacionadas à segurança on-line.

CYBERBULLYING

DEFINIÇÕES DISTINTAS. Alguns casos de cyberbullying são claramente identificáveis, dada a linguagem e a tática utilizadas para importunar e/ou intimidar uma vítima on-line. No entanto, dada a gama de comportamentos problemáticos/prejudiciais envolvidos, algumas vezes pode ser difícil apontar com precisão quando uma ação cruza a linha de má conduta para uma ofensa1 mais séria—e possivelmente criminosa. Não obstante, os pesquisadores geralmente caracterizam o cyberbullying como ações que utilizam um meio tecnológico para intimidar ou transmitir uma intenção de prejudicar. Com frequência a comunicação envolve a repetição de atos e um desequilíbrio de poder entre a vítima e o perpetrador. Em discussões de cyberbullying, a repetição implica que a comunicação seja repetida e o dano seja intencionalmente infligido—tipicamente não é uma ocorrência única e isolada. O desequilíbrio de poder refere-se amplamente à dinâmica que dá ao intimidador poder sobre a(s) vítima(s). Na forma tradicional de intimidação que ocorre pessoalmente, o desequilíbrio de poder frequentemente toma a forma de vantagem por força física, tamanho, ou outra vantagem estratégica. Na intimidação pela Internet, o desequilíbrio de poder pode ser conceitualizado de uma série de formas. Por exemplo, um intimidador pode ter maior familiaridade com a Internet do que a vítima. O intimidador também é capaz de preservar o anonimato: a força física não é necessária para manter o poder, uma vez que o intimidador cibernético é capaz de proteger sua identidade da(s) vítima(s) 1 Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. Computers in Human Behavior, 29(6), 2703-2711. 2 (Sabella et al, 2013). 3 Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26-32. No bullying na Internet, o desequilíbrio de poder pode ser conceitualizado em uma série de formas. Por exemplo, um intimidador pode ter uma maior familiaridade com a Internet do que a vítima. Segurança de Jovens na Internet: Riscos, Respostas e Recomendações de Pesquisa 3 por um período de tempo prolongado4. Essa habilidade de ocultar a identidade também é capaz de levar ao cyberbullying pessoas que não praticam bullying em contextos tradicionais. Adicionalmente, o fato de que o conteúdo no espaço cibernético é difícil ou impossível de deletar também pode contribuir para os sentimentos de impotência ou humilhação de uma vítima, o que, algumas vezes, podem desencoraja-la de buscar a ajuda de um adulto. (Adina Farrukh, 2014)

Redes Sociais

Atualmente a Internet faz parte das nossas vidas e todos utilizamos ou conhecemos alguém que utiliza uma ou várias Redes Sociais, que são websites que te permitem trocar informação, falar com outras pessoas, jogar e divertires-te através da Internet (Facebook, Twitter, MySpace, Google+, etc.). Utiliza as Redes Sociais da forma mais segura possível seguindo alguns conselhos que tornarão a tua navegação mais suave:

1. Coloca apenas informação que possa ser tornada pública sem riscos.
2. Não publiques fotografias tuas, dos teus amigos e da tua família em websites acedidos por gente que não conheces bem
3. Não publiques na Internet fotografias ou vídeos de ninguém sem o seu consentimento.

(Segura)

SPAM

São mensagens de correio eletrónico não solicitadas, normalmente associadas a publicidade, e que são muito suscetíveis de se associar a situações de phishing. Os emails para listas ou as cadeias de solidariedade são formas de angariar novos endereços onde se vai poder difundir uma atividade maliciosa. Como precaução deve verificar sempre a origem deste tipo de mensagens e a sua credibilidade.

Phishing

Método suportado no correio eletrónico através do qual um indivíduo se faz passar por alguém conhecido ou por uma entidade com o objetivo de se apropriar de informação que permita o acesso não autorizado a sistemas, informações e a contas bancárias. Como exemplo, os casos em que se criam páginas falsas de entidades bancárias e, no processo de entrada nas contas, se solicita a atualização de dados online, como códigos de acesso ou números de contribuinte. As instituições fidedignas não procedem desta forma para atualização de dados. O propósito deste ato fraudulento é aceder a informação pessoal que permita aos burlões aceder à sua identidade e debitar contas ou cometer crimes em seu nome. (Segurança na Internet nº8)

Segurança da Internet no Telemóvel

Um telemóvel, tal como os computadores, também é vulnerável a certos perigos, como os do phishing, SPAM, roubo de identidade e cyberbullying, pelo que se aplicam algumas regras:

1. Câmaras fotográficas – A câmara fotográfica não constitui, por si, um perigo, mas a utilização por parte de indivíduos menos bem-intencionados já o pode ser. Se alguém tirar uma fotografia a uma pessoa sem a sua autorização (por exemplo, nuns balneários) e a colocar na Internet, isto constitui um ato de cyberbullying. •
2. Cyberbullying – O cyberbullying aplica-se aos telemóveis também, na medida em que é também possível receber uma mensagem (SMS), imagem (MMS), além de chamadas, cujo propósito seja o de intimidar, incomodar e/ou ameaçar, entre outros.
3. SPAM – Embora não seja, por si só, um perigo, o SPAM (mensagens de texto ou outras contendo informação/publicidade não solicitada) pode ser extremamente incomodativo, na medida em que podemos receber inúmeros SMS que não nos interessam, a diversas horas do dia. Contudo, tenha em atenção que o SPAM também pode conter phishing, pelo que deverá tratar estas mensagens com cuidado e reserva. Módulo 3 - Navegar em Segurança: Direitos e Deveres 20
4. Bluetooth – Pode, se o utilizador não for cuidadoso, ser um meio de invasão da privacidade. Se deixar o Bluetooth ligado, é possível a terceiros aceder sem autorização às informações do seu telemóvel. Para evitar que isto aconteça, desligue esta funcionalidade depois de efetuar a transferência de dados. Quando está no modo "visível", o telemóvel ou PDA Bluetooth envia um sinal a indicar que está disponível para "emparelhar" com outro dispositivo Bluetooth e transmitir e receber dados. No entanto, um intruso que detete este sinal poderia igualmente tentar emparelhar com o seu dispositivo e aceder ilicitamente aos seus dados, para roubar o seu número de identificação pessoal (PIN). Poderá não ter a noção que o intruso, com o seu PIN, poderá roubar informações guardadas no seu dispositivo, incluindo listas de contactos, mensagens de correio eletrónico e mensagens de texto; Enviar mensagens de texto ou imagens não solicitadas para outros dispositivos Bluetooth; Aceder aos comandos do seu telemóvel , o que permitiria que o intruso utilizasse o seu telemóvel para fazer chamadas, enviar mensagens de texto, ler e escrever contactos na lista telefónica, escutar conversas e ligar à Internet; Instalar um vírus no seu dispositivo, que poderia provocar os mesmos danos que um vírus de computador — por exemplo, abrandar ou descativar o seu serviço, ou destruir e roubar informações; os criminosos também andam com detetores Bluetooth, à procura de telemóveis e PDAs para infiltrar, instalando potentes antenas em computadores portáteis, de forma a captar sinais Bluetooth a uma distância até perto de um quilómetro.
5. Vírus – Embora seja ainda pouco comum receber vírus no telemóvel, este perigo existe e terá tendência, a par das outras tecnologias da comunicação, a crescer com o tempo. Hoje em dia, é possível alguém mal-intencionado apagar remotamente dados de um telemóvel, desde que possua alguns dados a respeito do mesmo (nº de identificação, por exemplo). Os vírus já se propagam nos computadores de bolso (“palmtops”) e nos PDAs, pelo que é recomendável que tenha algum cuidado a transferir dados com esses equipamentos. (Aire, s.d.)

Segurança nas consolas de jogos

As consolas permitem a participação numa variedade de jogos e atividades, alguns dos quais pela Internet. De forma que, a questão da segurança on-line também se coloca. Destacamos as recomendações de segurança fornecidas pela Nintendo na utilização da consola Wii

Pais – Proteger a privacidade dos seus filhos

• Antes de deixar os seus filhos utilizarem a consola Wii, recomendamos vivamente que lhes explique a importância de não partilharem qualquer informação pessoal com desconhecidos. Informe-os de que não devem usar nenhuma informação pessoal nos nicknames na consola Wii, nos nomes de utilizador das salas de chat, nos nomes dos Miis ou quaisquer outros aspetos dos Serviços oferecidos através da consola Wii. Explique-lhes o perigo de receberem mensagens de desconhecidos ou da comunicação com desconhecidos. •. Deve vigiar as crianças sempre que estas utilizarem a consola Wii e ajudá-las na configuração da consola Wii. Se, em qualquer altura, pretender que os seus filhos deixem de usar as características interativas ou on-line da consola Wii, pode restringir o acesso aos serviços on-line da Wii utilizando o Controlo Parental.

Proteger a privacidade da sua informação pessoal quando utiliza a consola Wii

•. Nunca divulgue informações pessoais, tais como o seu primeiro e último nome, número de telefone, data de nascimento, idade, endereço eletrónico ou morada, quando comunicar com desconhecidos ou usar qualquer um dos serviços oferecidos na sua consola Wii.

•. Se utilizar as funções de mensagem da consola Wii, deve ter em conta que a Nintendo pode controlar a sua utilização e partilha de informação (i) como previsto na lei (ii) quando necessário para proteger a sua empresa, clientes e empregados ou (iii) quando necessário para fornecer os seus serviços.

•. Se decidir fornecer informações pessoais a outros sites da Internet, a partilha dessa informação estará sujeita à política de privacidade dessa empresa, e não às políticas de privacidade da Nintendo. Seja prudente ao fornecer qualquer informação pessoal a terceiros através dos serviços de rede oferecidos na sua consola Wii.

• A sua consola Wii pode guardar determinada informação pessoal no seu Comando Wii, por isso tenha em atenção que ao usar o Comando Wii noutra consola que não seja a sua, é possível que determinada informação pessoal seja partilhada com essa consola.

•. Para sua proteção, antes de vender, dar ou de algum modo transferir a sua consola Wii, por favor certifique-se que limpou e removeu da sua consola Wii, de forma segura, toda a sua informação pessoal, incluindo fotografias ou mensagens do Quadro de Mensagens da Wii e toda a informação sensível armazenada no disco duro da consola Wii. (Aire, s.d.)

Riscos associados à Internet

Cada vez mais na vida quotidiana o Homem está ligado a este invento. Nos empregos trabalha-se com a internet, nas escolas utiliza-se a internet, em casa usa-se a internet e até nos hospitais a internet é necessária. Se hoje em dia já se está neste patamar, em que já existem pessoas que trabalham em casa pela internet sem se deslocarem para o emprego, pessoas que estudam pela Internet, brincam e namoram.

A preocupação com os perigos da utilização da internet pode ser agrupada em três categorias:

♣ Conteúdos impróprios, legais ou ilegais, tais como a pornografia, pornografia infantil, violência, ódio, racismo e outros ideais extremistas, estão facilmente disponíveis a crianças e jovens através de uma grande variedade de dispositivos. Para além de poderem ser inadequados e prejudiciais a um desenvolvimento harmonioso, podem mesmo ofender os padrões e valores segundo os quais pretende educar os seus filhos ou educandos.

♣ Contactos potenciais por parte de pessoas mal-intencionadas, que usam o email, salas de chat, instant messaging, fóruns, grupos de discussão, jogos online e telemóveis para ganharem acesso fácil a crianças e jovens e que poderão desejar fazer-lhes mal e enganá-las, representam uma verdadeira ameaça.

♣ Comércio - práticas comerciais e publicitárias não- éticas que, não distinguindo a informação da publicidade, podem enganar crianças e jovens, promover a recolha de informações que violam a sua privacidade e promover a venda direta a crianças, atraindo-as a fazerem compras não autorizadas.

Perigos e Fraudes na Internet

Uma pessoa quando se faz passar por outra muitas das vezes utiliza o e-mail, para persuadir o verdadeiro dono do computador a fornecer informação útil para que ele possa fazer algum tipo de fraude. É preciso ter em mente que neste tipo de situações, o conhecimento empírico é importante, pois para qualquer tipo de abordagem que nos seja feita, temos sempre que estar vigilantes e nunca fornecer qualquer tipo de informação que possa colocar em risco a nossa privacidade ou segurança. É crucial não revelar qualquer tipo de informação. Os jovens poderão correr riscos também em conversas nos chats, no MSN, Facebook entre outros, uma vez que através destes podem manter conversas com pessoas de identidade simulada, pois nada os obriga a dar a sua verdadeira identidade. Os jovens poderão interagir com essas pessoas, fornecendo informações pessoais, muitas das vezes de extrema importância, fazendo com que a pessoa do outro lado fique a conhecer e saber algumas coisas importantes, desde rotinas diárias, gostos, quando estão ou não sozinhos em casa, entre outros. Essas informações fornecidas de forma pouco consciente poderão levar a que pessoas menos bem-intencionadas tenham condições de arquitetar algum crime ou ilegalidade.

e-Drugs

Como estamos em plena era digital, tem-se vindo a falar cada vez mais de uma droga eletrónica que os adolescentes hoje em dia utilizam como muita frequência mas sem qualquer tipo de racionalização e sem consciência que ela exista, estamos a falar das drogas eletrónicas/e-drugs que se caracteriza por ser uma droga sonora, ou seja, é caracterizada pela emissão de vários sons em cada ouvido simuladamente e que vão desencadear reações no cérebro podendo deixar a pessoa em questão muito descontraído ou por outro lado extremamente eufórico. “Certamente qualquer estímulo repetitivo aplicado com rotina poderá ser, em grau maior ou menor, uma fonte de dependência”, afirma o neurorradiologista e coordenador do Instituto do Cérebro do Einstein, Dr. Edson Amaro Jr. Este tipo de drogas, é comercializado em sitio da internet especializados em que o seu uso é limitado, e neste momento estas drogas são categorizadas em: doses espirituais, sedativas, dieta ou sexuais.” Estamos cada vez mais 44 próximos de uma geração em que alguns indivíduos entrarão na dependência eletrónica”, como afirma o Dr. Edson Amaro Jr.

“O curioso é que esta frase pode parecer chocante para quem lê a respeito das e-drugs, mas pode não representar nenhuma novidade para quem conhece ou vive os efeitos da internet”, afirma o médico. “Porém, a questão das e-drugs é diferente do uso da internet. Não se trata da utilização de computadores na rotina diária e o seu impacto pessoal ou na sociedade, mas sim da utilização de sistemas computacionais que interage com os sentidos e que seguem teorias de resposta cerebral”.

Este tipo de drogas funciona como uma hipnose acústica, que pode levar a sensações de prazer ou pelo contrário as sensações chatas e angustiantes, o que já acontece com as ditas drogas convencionais. Uma e-drug caracteriza-se por uma ação neurológica que é provocada por emissão de vários sons diferentes em cada ouvido, causando reações adversas no ouvinte, podendo levar à hipnose acústica. O principal meio de proliferação são as redes sociais, e a rapidez com que conquista os utilizadores despertou o alerta de certos setores. (Cepeda, 2012)



Figura 1 - E-Drugs

A Dependência da Internet e os Efeitos na Saúde

A Dependência da Internet tem vindo a ser considerada uma das novas formas de adição, na atualidade. Integrada no grupo das dependências comportamentais tem vindo a ocupar um lugar de destaque no ranking das adições. Na opinião de vários autores, o termo mais utilizado nesta área é a “Dependência da Internet”. Existem, no entanto, outros termos que são utilizados para descrever esta mesma situação, dos quais salientamos: transtorno de Dependência da Internet, uso patológico da Internet, abuso da Internet, uso compulsivo da Internet, compulsão ou ainda dependência virtual. A Dependência da Internet foi pesquisada pela primeira vez em 1996. Foram examinados mais de 600 casos de utilizadores que apresentavam sinais clínicos de dependência, identificados por uma versão adaptada dos critérios do DSM-IV (Diagnostic and Statistical Manual of Mental Disorders - IV) para o jogo de azar (Young, 1996). Este tema tornou-se alvo de atenção após a apresentação do artigo “Internet addiction: The emergence of a new clinical disorder” (Young, 1996), no encontro anual da APA (American Psychological Association). Desde então, têm sido várias as investigações relacionadas com esta temática.

A Dependência da Internet é um distúrbio comportamental que leva o indivíduo a passar para segundo plano todas as suas responsabilidades pessoais, familiares, sociais e profissionais. Caracteriza-se por ser uma dependência psicológica. É uma patologia grave, que pode condicionar de forma traumática e violenta a vida de milhares de seres humanos e das respetivas famílias. Inclui componentes como a preocupação excessiva com a Internet, alterações do humor, sintomas de abstinência, stresse, mentiras acerca do tempo online, conflitos e recaídas, como qualquer outra adição.

Sintomas

Tal como outras dependências comportamentais também a Dependência da Internet pode causar danos físicos e emocionais. Os vários sintomas quando detetados na pessoa dependente deverão ser bem avaliados. Entre os sintomas físicos, estão incluídos a taquicardia, a secura da boca e alguns tremores. A longo prazo, a maior frequência do dependente em manter-se online no computador provoca problemas como comprometimento da postura, dores musculares, lesões por esforço repetitivo (tendinite), obesidade devido a má alimentação e alterações na visão. Também pode surgir cansaço devido às madrugadas passadas online, assim como insónias. Do lado psíquico, a incapacidade de concentração, a agitação, a angústia por estar longe de um computador, estão entre os problemas apresentados. Todas estas características comprometem a pessoa em causa de diversas formas, originando baixo rendimento escolar ou profissional, perda do interesse pelas interações sociais arriscando a perda de uma relação significativa quer seja pessoal, profissional ou educacional. As pessoas ficam sem motivação para fazer algo que não seja utilizar a Internet sendo a autoestima muito afetada. (Alves, 2014)

# Bibliografia

Adina Farrukh, R. S. (2014). Segurança de Jovens na Internet: Riscos, Respostas e Recomendações de Pesquisa. *Center of* Technology *Innovation at bookings*.

Aire, E. S. (s.d.). *Módulo 3 Navegar em Segurança Direitos e Deveres*. Obtido de http://esmaa-m.ccems.pt/file.php/1/docs-seguranca/Navegar\_em\_seguranca\_direitos\_e\_deveres.pdf

Alves, P. A. (2014). *A Dependência da Internet.* Coimbra.

Cepeda, C. S. (2012). *Dissertação - Criança e In/Segurança na internet: estudo de caso no 3º Ciclo do Ensino Básico.* Bragança.

Correia, F. L. (2011). *Internet – sala de estudo virtual.* TESE DE DOUTORAMENTO.

Segura, I. (s.d.). Navegar na net sem problemas.

*Segurança na Internet nº8.* (s.d.). Obtido de http://www.rcc.gov.pt/novaaprendizagem/nl/Documents/Guia%20@prender\_8.pdf