

# SEGURANÇA NA INTERNET

## Guia para Professores

## Índice

<b>1. Segurança na Internet e os vários ciclos de ensino</b>	<b>3</b>
1.1. Pré-Escolar	3
1.2. Primeiro Ciclo	5
1.3. Segundo Ciclo do Ensino Básico	7
1.4. Terceiro Ciclo do Ensino Básico e Ensino Secundário	9
<b>2. Pesquisar</b>	<b>11</b>
2.1. Preparar a pesquisa – o que pesquisar e que ferramentas utilizar?	12
2.2. Recolher informações – que informação seleccionar e quais os critérios a usar?	13
2.3. Avaliar a informação – qual a fiabilidade e fidedignidade da informação?	14
<b>3. Comunicar</b>	<b>16</b>
3.1. Correio electrónico – como criar e usar contas em segurança	17
3.1.1. Não se deixe enganar por falsas mensagens de correio electrónico	18
3.1.2. Nova tecnologia de identificação do remetente ajuda a manter a confiança no correio electrónico	19
3.1.3. Ajude a evitar vírus informáticos que se espalham através do correio electrónico	20
3.1.4. O que deve fazer e o que não deve fazer ao lidar com mensagens de correio electrónico suspeitas	21
3.2. As mensagens instantâneas – garantir contactos seguros	22
3.3. Regras de conduta na Internet – evitar situações de conflito	24
<b>Ligações Úteis</b>	<b>26</b>

## 1. Segurança na Internet e os vários ciclos de ensino

Para melhor orientarmos os nossos alunos quanto ao uso que fazem da Internet, devemos ter em conta, por um lado, as diferentes fases pelas quais os alunos passam, por outro lado, os riscos inerentes à utilização desta ferramenta e, por outro lado ainda, as medidas que nos podem ajudar a minimizar esses riscos. Quer os nossos alunos estejam agora a dar os primeiros passos na Internet, quer estejam já muito habituados a utilizá-la, nós, enquanto professores, podemos ajudá-los a avançar com mais segurança nesse mundo “virtual”.

À medida que vão crescendo e passando por diferentes fases das suas vidas, os alunos têm características e interesses diferentes, o que os torna mais vulneráveis a determinados perigos.

Apresentamos-lhe, nas secções que se seguem, informações e sugestões para que fique a saber mais sobre a segurança na Internet para alunos de diferentes níveis de escolaridade.

Poderá assim preparar melhor as aulas em que utiliza a Internet como recurso pedagógico e ficar mais alerta para os temas de maior importância em cada faixa etária.

### 1.1. Pré-Escolar

No Pré-escolar vamos imaginar, descobrir e explorar em segurança.

A educação pré-escolar é a primeira etapa da educação básica no processo de educação ao longo da vida, sendo complementar da acção educativa da família. Neste nível de escolaridade temos como grande meta promover o desenvolvimento pessoal e social da criança, bem como contribuir para a igualdade de oportunidades e para o sucesso das suas aprendizagens.

As novas tecnologias fazem parte do conjunto de recursos que permitem estimular o desenvolvimento global das crianças, e a Internet oferece-nos um conjunto de funcionalidades que, devidamente utilizadas, podem ajudar as crianças a obter uma melhor compreensão do mundo. Ainda que nestas idades as crianças tenham uma capacidade de atenção limitada para as actividades on-line, as imagens e os sons da Internet podem estimular a sua imaginação e enriquecer as suas experiências.

Nesta fase, os professores, assim como os pais, devem acompanhar as crianças nas suas visitas à Internet, navegando em sítios *Web* dedicados aos mais pequenos ou jogando on-line. Enquanto professores, é fundamental que tenhamos sempre a preocupação de ensinar os nossos alunos a fazerem uma utilização segura da Internet, supervisionando rigorosamente as suas reacções perante o que encontram on-line.

Para que possamos ajudar os nossos alunos a usufruir de todos os benefícios que a Internet pode trazer, é necessário ter em conta que também existem riscos que devemos minimizar. Deixamos-lhe, por isso, nove sugestões que podem aumentar o grau de segurança de utilização da Internet neste nível de escolaridade.

### Soluções de Segurança no Pré-Escolar

1. Acompanhe sempre os seus alunos nas suas visitas à Internet;
2. Adicione sítios aceitáveis à lista de *Favoritos* dos computadores da sua sala /escola, para criar um ambiente on-line personalizado e seguro para os mais pequenos.
3. Utilize motores de pesquisa destinados a crianças, ou motores de pesquisa com controlos para restrição de acesso.
4. Informe-se, junto do coordenador TIC da sua escola, sobre ferramentas de filtragem de conteúdos da Internet para usar como complemento, e não como substituto, da supervisão dos professores.
5. Ajude a proteger os seus alunos de janelas de publicidade ofensivas, com software que bloqueia janelas *pop-up*. Peça ao coordenador TIC da sua escola que instale esse software nos computadores.
6. Nesta idade, nunca deixe que os seus alunos usem sozinhos serviços de mensagens instantâneas, correio electrónico, salas de chat ou fóruns de mensagens.
7. Comece desde cedo a ensinar aos seus alunos a importância da privacidade. Por exemplo, se um sítio *Web* encorajar as crianças a fornecerem os seus nomes para personalizar o conteúdo *Web*, sugira-lhes algumas alcunhas para utilização on-line que não revelem qualquer informação pessoal.
8. Não se esqueça que os mais velhos são sempre os modelos dos mais pequenos, pelo que deve fomentar comportamentos de segurança por parte dos alunos mais velhos e dos outros professores.
9. Envolver os pais nesta fase de exploração da Internet. Sugira-lhes actividades adequadas à faixa etária dos seus filhos, sítios dedicados a crianças, bem como sítios que abordem as questões de segurança na Internet.

## 1.2. Primeiro Ciclo

No 1º Ciclo vamos aprender a ler, a escrever e a navegar em segurança.

No 1.º Ciclo devemos proporcionar aos nossos alunos experiências de aprendizagem activas, significativas e diversificadas. Desde o início do Ensino Básico que devemos garantir aos nossos alunos oportunidades de desenvolvimento dos seus interesses, aptidões e capacidades, assim como promover uma realização individual em harmonia com os outros.

Para o conseguirmos, devemos procurar metodologias e estratégias de ensino, bem como actividades de aprendizagem, que favoreçam o desenvolvimento dos alunos numa perspectiva globalizante. A Internet, enquanto tecnologia de informação e comunicação, fornece-nos um manancial de recursos que, de forma cuidadosa, podemos usar em benefício das aprendizagens dos alunos.

Nestas idades, as crianças já conseguem seguir instruções no computador, utilizar o rato e o teclado, sentindo muitas vezes que já podem navegar e comunicar na Internet sem qualquer problema. Todavia, é de extrema importância acompanhar de perto o uso que fazem dessas ferramentas, uma vez que nesta faixa etária as crianças têm tendência a gostar de comunicar e partilhar, confiando por vezes demasiado nos outros.

Os professores assumem nesta fase da escolaridade um papel decisivo na formação dos comportamentos dos alunos em relação ao mundo que os rodeia, devendo por isso assegurar-se que o uso da Internet seja feito da forma mais segura possível. Para o ajudar, veja algumas sugestões de segurança que deve ter em conta quando estiver on-line com os seus alunos.

### Soluções de Segurança no 1º Ciclo

1. Crie uma lista de regras para utilização da Internet, com a colaboração de toda a turma.
2. Adicione sítios aceitáveis à lista de *Favoritos* dos computadores da sua sala /escola, para criar um ambiente on-line personalizado e seguro para os mais pequenos, e encoraje-os a visitar apenas sítios aprovados por si.
3. Utilize motores de pesquisa destinados aos mais pequenos ou motores de pesquisa com controlos para restrição de acesso.
4. Mantenha-se em locais da sala que lhe permitam visualizar e supervisionar facilmente as actividades dos seus alunos. Caso a disposição da sala não o permita, aborde a questão com o coordenador TIC da sua escola.

5. Informe-se, junto do coordenador TIC da sua escola, sobre ferramentas de filtragem de conteúdos para usar como complemento, e não como substituto, da supervisão dos professores.
6. Peça ao coordenador TIC da sua escola que instale nos computadores software bloqueador de janelas *pop-up*, para proteger os seus alunos contra publicidade ofensiva.
7. Ensine os seus alunos a não transferir software, música, ou ficheiros sem autorização.
8. Comece a ensinar aos seus alunos a importância da privacidade, alertando-os para que nunca revelem informações pessoais quando estiverem on-line.
9. Crie uma conta de correio electrónico partilhada pela turma e utilize-a, nas suas aulas em actividades de intercâmbio com outras turmas ou até com as famílias.
10. Utilize filtros de correio electrónico para bloquear mensagens de determinadas pessoas ou mensagens que contenham palavras ou frases específicas.
11. Deixe-os utilizar apenas salas de chat e fóruns de mensagens monitorizados, em sítios para crianças, bem conceituados.
12. Fale com os seus alunos sobre os seus amigos e as suas actividades on-line, tal como faria em relação às suas outras actividades no mundo real.
13. Nas suas aulas, comece a abordar as questões de sexualidade saudável, porque é muito fácil as crianças encontrarem on-line conteúdos para adultos ou pornográficos.
14. Encoraje os seus alunos a falarem consigo, ou com os pais, se alguma coisa ou alguém on-line os fizer sentir pouco à vontade ou ameaçados. Mantenha-se calmo e lembre-lhes que não terão qualquer problema se lhe contarem algo que se tenha passado on-line. Elogie o seu comportamento e encoraje-os a irem ter consigo caso volte a acontecer o mesmo. Obtenha informações adicionais sobre como lidar com predadores on-line e *cyberbullies*.

### 1.3. Segundo Ciclo do Ensino Básico

No 2º Ciclo vamos encontrar e compreender novos saberes em segurança.

O 2.º Ciclo traz um conjunto de novidades e situações novas para os alunos. Deixam de ter um só professor para passar a ter vários e passam a necessitar de conhecimentos em domínios cada vez mais específicos. É, neste momento, que começa o grande trabalho de equipa entre todos professores de uma turma para proporcionar o mais vasto e enriquecedor conjunto de experiências de aprendizagem.

Propõem-se actividades mais complexas, recorre-se mais a trabalhos de grupo e desenvolvem-se mais projectos do que até aqui. As tecnologias de informação e comunicação assumem-se, nesta altura, como um elemento quase indispensável à realização de tarefas escolares, desde a formatação de trabalhos à pesquisa de informação inerente à concretização dos mesmos.

Nestes anos da pré-adolescência ocorrem grandes alterações na vida dos alunos, que começam a ter mais curiosidade pelo mundo que os rodeia e a dar mais importância às relações com os amigos. Com esta idade, grande parte dos nossos alunos já pesquisa na Internet, transfere música, usa o correio electrónico, joga jogos on-line e adora comunicar com os seus amigos através de mensagens instantâneas (IM).

Enquanto professores devemos orientar a utilização da Internet, assegurando que os procedimentos de segurança são cumpridos e que os nossos alunos sabem quais são os comportamentos e atitudes promotores de segurança. Assim, deixamos-lhe algumas sugestões para aumentar a segurança dos seus alunos quando realizam actividades on-line.



#### **Soluções de Segurança no 2º Ciclo**

1. Crie uma lista de regras para utilização da Internet, com a colaboração de toda a turma.
2. Mantenha-se em locais da sala que lhe permitam visualizar e supervisionar facilmente as actividades dos seus alunos. Caso a disposição da sala não o permita, aborde a questão com o coordenador TIC da sua escola.
3. Informe-se junto do coordenador TIC da sua escola, sobre ferramentas de filtragem de conteúdos para usar como complemento e, não como substituto, da supervisão dos professores.
4. Peça ao coordenador TIC da sua escola que instale nos computadores software bloqueador de janelas pop-up, para proteger os seus alunos contra publicidade ofensiva.

5. Converse com os seus alunos sobre os seus amigos e as suas actividades on-line, tal como faria em relação às suas outras actividades no mundo real.
6. Deixe os seus alunos utilizar apenas salas de chat monitorizadas, em sites bem conceituados orientados para crianças, deixando bem claro que nunca devem aceitar encontrar-se pessoalmente com alguém que conheceram on-line.
7. Avise os seus alunos de que nunca devem revelar informações pessoais quando utilizam correio electrónico, salas de chat, ou serviços de mensagens instantâneas, nem tão pouco quando preenchem formulários de registo ou participam em concursos on-line.
8. Ensine os seus alunos que não devem transferir programas sem autorização, pois, inadvertidamente, podem estar a transferir spyware ou um vírus informático.
9. Explique aos seus alunos que ao retirarem texto ou imagens da Web podem estar a violar a lei dos direitos de autor. Mostre-lhes como citar adequadamente essas fontes.
10. Para que os seus alunos não participem em determinadas actividades sem o seu conhecimento no espaço da escola, fale com o Coordenador TIC sobre as possíveis restrições das suas contas de utilizador.
11. Encoraje os seus alunos a falarem consigo, ou com os pais, se alguma coisa ou alguém on-line os fizer sentir pouco à vontade ou ameaçados. Mantenha-se calmo e lembre-lhes que não terão qualquer problema se lhe contarem algo que se tenha passado on-line. Elogie o seu comportamento e encoraje-os a irem ter consigo caso volte a acontecer o mesmo. Obtenha informações adicionais sobre como lidar com predadores on-line e cyberbullies.
12. Converse com os seus alunos sobre pornografia on-line e oriente-os para bons sites sobre saúde e sexualidade.
13. Fale com os seus alunos sobre o que é um comportamento on-line responsável e ético. Não devem usar a Internet para espalhar boatos e intimidar ou ameaçar outras pessoas.
14. Certifique-se de que os outros professores das suas turmas estão alertados para importância destas questões. Sugira-lhes sites que falem destes temas e proponha-lhes projectos interdisciplinares que ajudem a educar os alunos para a segurança na Internet.

## 1.4. Terceiro Ciclo do Ensino Básico e Ensino Secundário

No 3º Ciclo e Secundário vamos investigar e analisar o mundo em segurança.

Esta última fase da escolaridade básica é, juntamente com o início do prosseguimento de estudos, um momento pautado por escolhas e pela tomada de decisão quanto a opções futuras. É imperativo garantir aos nossos alunos as oportunidades necessárias para que desenvolvam os seus interesses e alarguem os seus horizontes.

A Internet e outras tecnologias de informação e comunicação não constituem novidade para a maioria dos alunos nestes níveis de ensino. O recurso a estas ferramentas proporciona-lhes a aquisição de um conjunto de competências cada vez mais importante na sociedade actual, assim como, novas oportunidades para conhecer realidades diferentes das suas.

Os alunos já estão habituados a utilizar a Internet. Nestes níveis de ensino os alunos já transferem música, utilizam serviços de mensagens instantâneas (IM), correio electrónico, jogam jogos on-line e usam activamente motores de pesquisa para encontrar informações. O mais provável é que os rapazes forcem os limites e procurem sites de humor grosseiro, violência, jogos de azar, ou sites explicitamente para adultos, e que as raparigas gostem de conversar on-line, o que as torna mais susceptíveis a solicitações on-line de cariz sexual.

Numa fase em que a aprovação por parte dos colegas e a busca da independência guia muitos dos comportamentos que os alunos têm, é essencial que os professores continuem a orientá-los quanto à utilização da Internet. Leia algumas sugestões de segurança a ter em conta quando os seus alunos adolescentes utilizam a Internet.

### Soluções de Segurança no 3º Ciclo e Secundário

1. Com a colaboração dos alunos crie uma lista de regras para utilização da Internet. Deverá incluir os tipos de sites que não são permitidos usar nas aulas e instruções para comunicação on-line, o que inclui a comunicação em salas de chat.
2. Mantenha-se em locais da sala que lhe permitam visualizar e supervisionar facilmente as actividades dos seus alunos. Caso a disposição da sala não o permita, aborde a questão com o coordenador TIC da sua escola.
3. Informe-se junto do coordenador TIC da sua escola sobre ferramentas de filtragem de conteúdos para usar como complemento e, não como substituto, da supervisão dos professores.
4. Explique aos seus alunos que não podem transferir programas, música,

ou ficheiros sem autorização. Se partilharem ficheiros ou retirarem texto ou imagens da Web, podem estar a violar a lei dos direitos de autor.

5. Converse com os seus alunos sobre pornografia on-line e oriente-os para bons sites sobre saúde e sexualidade.
6. Fale com os seus alunos sobre o que é um comportamento on-line responsável e ético. Não devem usar a Internet para espalhar boatos e intimidar ou ameaçar outras pessoas.
7. Fale com os seus alunos sobre os jogos de azar on-line e os seus potenciais riscos, lembrando-lhes que é ilegal jogarem este tipo de jogos.
8. Certifique-se de que os seus alunos não efectuem transacções financeiras on-line, o que inclui encomendar, comprar ou vender um artigo.
9. Converse com os seus alunos sobre os amigos deles e as suas actividades on-line, tal como faria em relação às suas outras actividades no mundo real.
10. Ajude-os a protegerem-se contra o spam. Diga aos seus alunos para não revelarem os seus endereços de correio electrónico on-line, para não responderem a "junk mail" e para utilizarem filtros de correio electrónico.
11. Avise os seus alunos de que nunca devem revelar informações pessoais quando utilizam correio electrónico, salas de chat ou serviços de mensagens instantâneas, nem tão pouco quando preenchem formulários de registo ou participam em concursos on-line.
12. Procure saber quais são as salas de chat ou os fóruns de mensagens que os seus alunos visitam e com quem falam on-line. Insista para que usem salas de chat monitorizadas e para que se mantenham em áreas públicas das salas de chat. Deixe bem claro que nunca devem aceitar encontrar-se pessoalmente com alguém que conheceram on-line.
13. Procure estar atento aos Web sites que os seus alunos visitam, de modo a tentar saber se visitam sites com conteúdos ofensivos ou se colocam na Internet informações pessoais ou fotografias deles mesmos.
14. Encoraje os seus alunos a falarem consigo ou com os pais, se alguma coisa ou alguém on-line os fizer sentir pouco à vontade ou ameaçados. Mantenha-se calmo e lembre-lhes que não terão qualquer problema se lhe contarem algo que se tenha passado on-line. Elogie o seu comportamento e encoraje-os a irem ter consigo caso volte a acontecer o mesmo. Obtenha informações adicionais sobre como lidar com predadores on-line e cyberbullies.

**15.**Alerte os seus colegas para a importância destas questões. Sugira-lhes sites que falem destes temas e proponha-lhes projectos interdisciplinares que ajudem a educar os alunos para a segurança na Internet.

## 2. Pesquisar

Uma das melhores maneiras de ajudar os nossos alunos a usarem a Internet de forma segura é incorporando nas nossas aulas actividades com recurso à Internet.

Assim, ao aproveitarmos as potencialidades desta ferramenta para melhorar as aprendizagens dos alunos, vamos trabalhando com eles práticas de segurança.

Se queremos usar a WWW para pesquisas, então vamos mostrar a importância de usar boas técnicas de pesquisa, de selecção de informação pertinente e de avaliação da fiabilidade dos conteúdos encontrados.

Cada vez mais temos os meios necessários para, nas nossas aulas, realizarmos investigações recorrendo ao apoio das tecnologias. A pesquisa on-line processa-se dentro do inesgotável manancial de recursos que a Internet disponibiliza aos seus utilizadores, tornando possível o acesso a conteúdos produzidos por qualquer pessoa, em qualquer parte do mundo. Ao pesquisar on-line os utilizadores podem alargar os seus conhecimentos pessoais e comparar diferentes perspectivas de abordagem sobre determinado conteúdo ou assunto. Todavia, esta forma de pesquisa acarreta riscos, nomeadamente, ao nível de:

- Conteúdos ilegais (pornografia infantil, racismo, difamação, publicidade sobre drogas ilegais, ameaças);
- Conteúdos nocivos (pornografia e linguagem para adultos, violência, informação sobre seitas);
- Conteúdos falsos (dar por certa informação que é falsa).

Assim, torna-se importante preparar as pesquisas on-line que vamos realizar em aula, bem como, alertar os nossos alunos para algumas medidas de segurança.

## 2.1. Preparar a pesquisa – o que pesquisar e que ferramentas utilizar?

Actualmente, com um computador e um acesso à Internet facilmente acedemos a trabalhos que outros produziram e disponibilizaram na *World Wide Web* (WWW). Em termos educativos esta possibilidade de acesso à informação é extremamente importante e enriquecedora, sendo, por isso, fundamental escolher os serviços de pesquisa mais adequados.

Previamente à elaboração da pesquisa é necessário definir o que pesquisar:

- Escolher o tipo de pesquisa mais adequado às necessidades e limitações;
- Saber exactamente o que se pretende pesquisar;
- Definir palavras-chave no âmbito da pesquisa que se vai realizar;
- Adoptar critérios de pesquisa claros.

Para tal é necessário que os utilizadores adoptem estratégias claras de planificação, de recolha, de compilação e de pensamento crítico aquando da execução da pesquisa que pretendem efectuar.

Ainda na fase de preparação devemos ter em conta os objectivos da pesquisa e as características dos nossos alunos, para podermos decidir que ferramentas utilizar.

Para fazer face às exigências colocadas pelo enorme crescimento que a Internet alcançou nos últimos anos foram criados serviços específicos que procuram ajudar e orientar os cibernautas nas suas pesquisas na Internet, nomeadamente, os directórios e os motores de busca.

### **Características importantes dos directórios Web:**

- São listas organizadas por categorias e subcategorias de temas que o cibernauta pode visualizar, procurando os sítios que pretende, acedendo-lhes directamente;
- Já se encontram organizados por categorias e subcategorias de temas, não sendo possível a pesquisa por palavras-chave, como acontece com os motores de busca;
- Todas as entradas disponíveis num directório já foram anteriormente avaliadas por pessoas que as inscreveram dentro de uma categoria / subcategoria.

Os directórios assumem-se como uma boa ferramenta para os alunos mais novos, uma vez que podem evitar a navegação em sítios de conteúdo abusivo.

### **Características importantes dos motores de busca:**

- São ferramentas que permitem pesquisar os documentos existentes na WWW, com base em palavras-chave ou em expressões definidas pelo utilizador;
- Apresentam, de forma muito célere, um conjunto de recursos que, de outra forma, seriam muito difíceis de reunir tendo em conta a quantidade de informações disponibilizadas na Internet;
- Exigem critérios de pesquisa e de interpretação dos resultados mais definidos, uma vez que podem devolver sítios com conteúdos falsos, nocivos ou ilegais.

Os motores de busca adequam-se a solicitações de pesquisa mais exigentes, sendo, todavia, necessário definir com mais clareza os critérios da pesquisa e de selecção da informação.

## **2.2. Recolher informações – que informação seleccionar e quais os critérios a usar?**

Após ter preparado a sua pesquisa na Internet torna-se fundamental tomar decisões sobre **que informação seleccionar**.

Se optar por um directório, os recursos disponíveis já se encontrarão organizados por tema, facilitando, de certa forma, a selecção dos resultados obtidos. Quanto aos motores de busca, tendo em conta a quantidade de informação que pode devolver aquando da pesquisa, é importante:

1. Inserir na área de pesquisa a palavra, expressão ou conjunto de palavras sobre as quais pretende recolher informação e passados alguns momentos surgir-lhe-ão as páginas onde essas palavras foram identificadas.
2. Ler adequadamente os resultados, uma vez que as expressões pesquisadas podem estar incluídas quer no título, quer ao longo do conteúdo das páginas identificadas.

Podemos, então, otimizar as nossas pesquisas nos motores de busca se:

- Usarmos o sinal de adição (+) antes da palavra, indicando que essa palavra deve aparecer no texto;
- Colocarmos a expressão entre aspas (" ") para procurar por uma frase exacta;
- Indicarmos o país das páginas a pesquisar;
- Utilizarmos um maior número de palavras, restringindo mais a pesquisa;
- Recorrermos às opções de "pesquisa avançada", para proceder à filtragem dos resultados, onde podemos escolher a língua, o formato do documento, etc....

Quando fazemos uma pesquisa na Internet os resultados obtidos surgem através da apresentação de uma listagem de endereços. Estes são seguidos de um breve texto extraído da página no qual aparecem as palavras ou expressões pesquisadas. É de extrema importância analisar esse excerto, pois permite prever o contexto no qual os termos de pesquisa aparecem na página, evitando aceder a sites impróprios.

Para que possamos organizar a recolha de informação de forma sistemática, podemos usar uma grelha que ajude a estruturar a pesquisa que vamos efectuando, evitando que nos desorientemos na imensidão da informação disponível na Internet. Nessa grelha podemos registar:

- URLs dos sítios Web / páginas visitados
- Título do sítio Web
- Temas abordados
- Autoria
- Outras observações

Alguns dos sítios enumerados no motor de busca podem não ter qualquer interesse logo à partida, pelo que podem não ser considerados. Outros, porém, podem vir a ser extremamente úteis no trabalho que posteriormente vamos realizar com a informação recolhida e facilitar a consulta desses recursos no futuro.

### 2.3. Avaliar a informação – qual a fiabilidade e fidedignidade da informação?

Publicar documentos na *World Wide Web* é extremamente fácil e está ao alcance de qualquer utilizador da Internet. Qualquer pessoa pode colocar na Internet todo e qualquer tipo de informação, podendo esta nem sempre ser verdadeira ou fiável.

**A fiabilidade e veracidade da informação** devem ser acauteladas sob pena de os alunos trabalharem sobre informações que não correspondem à realidade. Como o fazer?

1. É importante que a informação recolhida num sítio possa ser confirmada noutra(s) sítio(s) como forma de lhe dar consistência e maior credibilidade.
2. A informação encontrada nos directórios, porque avaliada antes de ser colocada nas respectivas categorias e subcategorias, pode garantir algum grau de credibilidade.
3. A utilização de sítios Web credíveis onde sejam fornecidas hiperligações para outros sítios é também outra das estratégias que podemos utilizar com os nossos alunos.
4. Pesquisar em sítios Web que, à partida, são idóneos em termos dos conteúdos que tornam públicos. Temos como exemplo as instituições educativas, que se identificam através do domínio .edu. Todavia, por si só, isto não significa uma certeza absoluta sobre a qualidade da informação veiculada.

Outros domínios comuns são os seguintes:

**edu** - educação  
**com** - organizações comerciais  
**eu** - União Europeia  
**pt** - Portugal  
**org** - organizações sem fins lucrativos  
**net** - empresas de telecomunicações e ISP  
**gov** - governo dos Estados Unidos da América

Na fase da avaliação dos resultados das pesquisas, o papel do professor é essencial para certificar, confirmar e avaliar os conteúdos consultados. Desenvolver nos alunos espírito crítico face à informação a que acedem na Internet é um ingrediente indispensável para que possam construir o seu próprio conhecimento, tendo como ponto de partida as informações recolhidas. Devemos fomentar nos nossos alunos a capacidade crítica em relação às fontes onde vão pesquisar, pedindo que façam questões tão simples como:

- Quem é o autor desta informação?
- Em que data foi publicada?
- A informação é factual?
- A informação resulta da opinião pessoal de alguém?
- Que garantias me são dadas de que posso confiar nesta informação?

Para os ajudar nesta tarefa, pode pedir-lhes que preencham uma lista de verificação sobre os sites consultados, na qual constem as seguintes questões:

- O conteúdo é fidedigno?
- A origem do conteúdo é conhecida?
- A informação não contém erros?
- A informação é relevante para o grupo etário para o qual foi concebido?
- Os textos e mensagens são facilmente legíveis?
- Os textos e mensagens são claros e cientificamente correctos?
- Os autores são de confiança em termos científicos?
- Inclui informação acerca da última actualização?

### 3. Comunicar

A Internet desenvolve novos modos de socialização e comunicação, destacando-se o envio de mensagens através do correio electrónico para colegas e amigos em todas as partes do mundo, e a troca de ideias, em tempo real, através dos chats.

No entanto, estas funcionalidades da Internet, que tanto interesse e motivação despertam nos mais novos, precisam de ser usadas de forma segura, a fim de evitar situações de risco. Devemos, por isso, acautelar-nos quanto aos contactos que se estabelecem na Internet, tendo em conta que:

- As diversas formas de contacto (chats, fóruns, correio electrónico, páginas *Web*) implicam riscos e medidas de precaução diferentes;
- O envio de ficheiros e a troca de informações podem ser mal intencionados;
- Os utilizadores podem ser anónimos e/ou fazer uso de falsa identidade, o que leva a que seja um lugar ideal para predadores on-line.

Se vamos usar a Internet para comunicar, essa será uma excelente oportunidade para pôr em prática as regras de privacidade, de convivência na Internet, alertando-os também para os riscos e cuidados a ter no que concerne a contactos com outras pessoas.

Hoje podemos usar estas ferramentas de comunicação na sala de aula, para proporcionar momentos de discussão que fomentam interacções promotoras de colaboração e, simultaneamente, para habituar os nossos alunos a terem comportamentos de segurança na Internet.

### 3.1. Correio electrónico – como criar e usar contas em segurança

A utilização do correio electrónico permite a realização de várias tarefas educativas.

Algumas das actividades que se podem desenvolver através da utilização do correio electrónico são, entre outras:

- Comunicar com os seus alunos, enviando apontamentos e fichas a qualquer momento;
- Receber os trabalhos realizados pelos seus alunos e enviar-lhes os seus comentários;
- Realizar trabalhos colaborativos com alunos de outras escolas;
- Utilizar as ferramentas de comunicação síncrona (chat's) ou grupos de discussão.

Neste momento é de grande importância criar contas seguras, nomeadamente no que diz respeito ao nome de utilizador e à definição da palavra passe. A correcta definição destes elementos pode evitar situações de perigo, pelo que deve ter em conta os seguintes aspectos:

- O nome de utilizador não deve conter informação pessoal;
- As palavras passe devem ter uma extensão de 8 caracteres ou mais, embora o ideal seja terem 14 ou mais caracteres;
- Quanto maior for a variedade de caracteres na sua palavra passe, mais difícil se torna descobri-la, pelo que deve combinar letras, números e símbolos;
- Devemos usar palavras e frases que sejam fáceis de recordar, mas difíceis de descobrir por outra pessoa.

Uma vez criada a conta de correio electrónico, é importante saber como a **usar de forma segura**. O correio electrónico é o meio privilegiado daqueles que pretendem propagar software nocivo e fazer fraudes on-line.

Muitos dos vírus informáticos e outro software nocivo espalham-se através dos anexos do correio electrónico (os ficheiros enviados juntamente com uma mensagem). Se um ficheiro anexo a uma mensagem de correio electrónico contiver um vírus, este é geralmente activado no momento em que abrimos o ficheiro anexo (normalmente com um duplo clique no ícone do anexo). Independentemente do programa de correio electrónico que utilizamos, podemos evitar a propagação de alguns vírus seguindo algumas regras básicas:

- Não abrir qualquer anexo, excepto se conhecermos o remetente e estivermos à espera desse anexo;
- Quando recebemos mensagens com um anexo de alguém que não conhecemos, devemos eliminá-las de imediato;
- Ter e manter actualizado um software antivírus;
- Utilizar filtros de spam para ajudar a bloquear correio electrónico indesejado, muito do qual contém anexos perigosos.

### 3.1.1. Não se deixe enganar por falsas mensagens de correio electrónico

Se receber uma oferta por correio electrónico que parece demasiado boa para ser verdade, provavelmente é mesmo. As burlas existem há séculos, mas a sua popularidade está a aumentar porque a Internet torna-os fáceis de espalhar.

Muitas formas de burla vão levá-lo a reencaminhar mensagens de correio electrónico sobre falsos vírus ou outras histórias inventadas. Estas mensagens de correio electrónico fazem perder tempo, obstruem as caixas de correio e causam embaraço quando se prova que não são verdadeiras. No entanto, existe um tipo de fraude mais insidiosa que pode acabar por custar muito dinheiro.

#### **Fraudes de pagamento antecipado**

Uma fraude de pagamento antecipado é um esquema que o atrai com uma falsa promessa de grandes somas de dinheiro em troca de pouco ou nenhum esforço da sua parte. Assim que está profundamente envolvido no esquema, pedem-lhe que pague certas quantias de dinheiro para acelerar o processo. Acaba por não receber um tostão.

Eis alguns exemplos das fraudes de pagamento antecipado mais populares:

- Um governo estrangeiro gostaria de ter a sua ajuda na transferência de fundos e vai pagar-lhe uma comissão choruda se aceitar.
- Vai receber milhões de dólares de herança de um parente de quem não se recorda.
- Ganhou um prémio ou uma lotaria (talvez de um país estrangeiro) em que não se lembra de apostar.

#### **Como detectar uma fraude**

Se pensar que uma mensagem de correio electrónico que recebeu é um esquema, um sítio a consultar é a lista de exemplos das páginas de referência

de burlas (The Urban Legends Reference Pages). No entanto, estes esquemas podem ter milhares de formas diferentes.

Eis mais sete sinais reveladores de um esquema:

1. Não conhece a pessoa que lhe enviou a mensagem.
2. Prometeram-lhe somas não declaradas de dinheiro, por pouco ou nenhum esforço da sua parte.
3. Pedem-lhe para fornecer uma quantia antecipada para actividades duvidosas, uma taxa de processamento, ou para pagar os custos de aceleração do processo.
4. Pedem-lhe para fornecer o número da sua conta bancária, ou outras informações financeiras pessoais, e o remetente oferece-se para depositar lá dinheiro.
5. O pedido tem um tom de urgência.
6. O remetente pede repetidamente que actue com confidencialidade.
7. O remetente oferece-se para lhe enviar fotocópias dos certificados governamentais, informação bancária, ou outras "provas" de que a sua actividade é legítima (são falsas).

### 3.1.2. Nova tecnologia de identificação do remetente ajuda a manter a confiança no correio electrónico

Em tempos elogiado como uma revolução na comunicação pessoal e global, o correio electrónico já não é tão simples e amigo do utilizador como era. O aumento do número de mensagens não-solicitadas (ou "spam") e o aumento das ameaças ao correio electrónico por fraudes como o "phishing" (tentativa de usar o correio electrónico para roubar dados de identidade) contribuíram para abalar a confiança que as pessoas depositavam no correio electrónico.

Em resposta, as empresas de tecnologias inovadoras estão a investir a toda a força contra os criadores de spam e de fraudes propagadas por correio electrónico, com tecnologias de autenticação do correio electrónico.

#### **Nova barra de ferramentas para ajudar a lançar avisos contra tentativas de phishing**

O spam e o phishing são ameaças sérias aos utilizadores de tecnologias informáticas em todo o mundo, e é importante que as empresas que apostam

na inovação tecnológica trabalhem em cooperação para ajudarem a resolver destes problemas.

As empresas de telecomunicações continuaram a trabalhar com outras organizações mundiais para melhorar as tecnologias de autenticação de correio electrónico e outras soluções anti-spam, incluindo instituições dos sectores educativo, legislativo e judicial, de forma a que se possa restaurar a confiança dos utilizadores de correio electrónico de todo o mundo.

### 3.1.3. Ajude a evitar vírus informáticos que se espalham através do correio electrónico

Muitos dos vírus informáticos e outro software nocivo mais comum espalham-se através dos anexos do correio electrónico — os ficheiros são enviados juntamente com uma mensagem de correio electrónico. Se um ficheiro anexo a uma mensagem de correio electrónico contiver um vírus, este é geralmente activado no momento em que abre o ficheiro anexo (normalmente com um duplo clique no ícone do anexo). Independentemente do programa de correio electrónico que utiliza ou da versão do sistema operativo que está a executar, pode ajudar a evitar a propagação de alguns vírus seguindo algumas regras básicas.



#### **Cinco sugestões para lidar com anexos de e-mail**

Siga estas orientações básicas quando receber um anexo numa mensagem de correio electrónico, independentemente do programa de correio electrónico que utiliza:

1. Não abra qualquer anexo, excepto se conhecer o remetente e estiver à espera desse anexo.
2. Se receber uma mensagem de correio electrónico com um anexo de alguém que não conhece, deve eliminá-la de imediato.
3. Utilize software antivírus e mantenha-o actualizado.
4. Se tiver de enviar algum anexo numa mensagem de correio electrónico para alguém, informe o destinatário de que lhe enviará o ficheiro, para que este não o confunda com um vírus.
5. Utilize filtros de spam para ajudar a bloquear correio electrónico indesejado, muito do qual contém anexos perigosos.

### **Aviso de segurança**

Tenha sempre cuidado antes de clicar em **Executar**, uma vez que isso poderá instalar um vírus ou outro programa potencialmente perigoso.

#### **3.1.4. O que deve fazer e o que não deve fazer ao lidar com mensagens de correio electrónico suspeitas**

A maioria dos esquemas de phishing são enviados por correio electrónico. Ao seguir estas linhas de orientação, pode ajudar a proteger-se destes esquemas.

**Comunique a recepção de correio electrónico suspeito.** Se suspeitar que recebeu correio electrónico de phishing destinado a furto-lhe a sua identidade, comunique a recepção da mensagem à organização cujo nome foi utilizado ou adulterado. Contacte a organização directamente – e não através da mensagem de correio electrónico que recebeu – e peça confirmação. Se preferir, ligue para o número gratuito da organização (se existir um) e fale com um representante do departamento de assistência ao cliente. Também deverá comunicar a recepção da mensagem às autoridades competentes. Se achar que recebeu uma mensagem de correio electrónico de phishing, não responda à mesma.

**Não corra riscos: evite clicar em ligações incluídas em mensagens de correio electrónico.** Muitas vezes, as ligações em mensagens de correio electrónico de phishing levam-no directamente para sites fictícios onde poderá, involuntariamente, transmitir informações pessoais ou financeiras a burlões. Evite clicar em ligações incluídas em mensagens de correio electrónico, a não ser que tenha a certeza do que está a fazer. Mesmo que a barra de endereços mostre o endereço Web correcto, não se deixe enganar. Os burlões têm ao seu dispor diversas formas de apresentar um URL falso na barra de endereços do seu browser.

**Escreva os endereços directamente no seu browser, ou utilize os atalhos na sua pasta de Favoritos.** Se precisar de actualizar as suas informações de contas bancárias ou de alterar a sua palavra-passe, visite o Web site utilizando a sua pasta de Favoritos, ou escrevendo o URL directamente no browser.

**Verifique o certificado de segurança antes de introduzir informações financeiras ou pessoais num Web site.** Antes de introduzir informações financeiras ou pessoais num Web site, certifique-se de que o site é seguro. No Internet Explorer e no Firefox, pode fazê-lo verificando o ícone de cadeado amarelo na barra de estado, como se vê no exemplo abaixo.

O cadeado fechado significa que a Web site utiliza encriptação para ajudar a proteger quaisquer informações pessoais confidenciais que introduza, como o número do seu cartão de crédito, dados que o identificam, ou detalhes de pagamentos. É importante referir que este símbolo não precisa de aparecer em todas as páginas de um site, mas apenas nas páginas onde são solicitadas informações pessoais. Infelizmente, mesmo o símbolo do cadeado pode ser falsificado. Para ajudar a aumentar a sua segurança, clique duas vezes sobre o ícone para visualizar o certificado de segurança do site. O nome que se segue a **Emitido para** deve corresponder ao nome do site. Se o nome diferir, pode estar num site falso, também designado como site "spoofed", ou com conteúdos ocultos. Se não tem a certeza da legitimidade do certificado, não insira qualquer informação pessoal. Jogue pelo seguro e saia do site.

**Conselho:** Se não vir a barra de estado na parte inferior da janela do seu browser, clique em **Ver** na parte superior do browser e, depois, seleccione **Barra de estado** para activá-la.

**Não introduza informações pessoais ou financeiras em janelas pop-up.** Uma técnica comum de phishing consiste em lançar uma janela pop-up falsa quando se clica numa ligação incluída numa mensagem de correio electrónico de phishing. Para tornar a janela pop-up mais convincente, esta poderá ser apresentada sobre uma janela em que confia. Mesmo que a janela pop-up pareça ser oficial ou afirme ser segura, deverá evitar introduzir informações confidenciais, pois não há maneira de verificar o certificado de segurança. Feche as janelas pop-up clicando no X vermelho que se encontra no canto superior direito (um botão "cancelar" poderá não funcionar como seria de esperar).

**Actualize com frequência o software do seu computador.**

### 3.2. As mensagens instantâneas – garantir contactos seguros

Os sistemas de mensagens instantâneas (geralmente denominados IM) são métodos de comunicação on-line semelhantes ao correio electrónico, mas mais rápidos.

O MSN Messenger é uma das ferramentas da Internet mais utilizadas pelos jovens cibernautas. Apesar de a utilização desta ferramenta em termos educativos não ser muito comum, a sua implementação apresenta aspectos positivos que não se podem, nem devem, descurar em termos pedagógicos, tais como:

- O estabelecimento de interações entre os participantes;
- O aumento da literacia tecnológica dos alunos, ao utilizarem uma ferramenta tecnológica em contexto;
- A possibilidade de arquivar na íntegra a discussão tida, permitindo ao professor uma análise e uma avaliação dos contributos feitos pelos alunos, quer em termos de qualidade, quer de quantidade.

Por vezes, as pessoas referem-se às conversas através de mensagens instantâneas como "chatting", mas os sistemas de "chat" e as mensagens instantâneas não são a mesma coisa. As mensagens instantâneas implicam uma conversa entre duas ou mais pessoas listadas nos seus contactos, enquanto que os chats são conversas numa "sala de chat" da Internet, aberta a todas as pessoas.

Comunicar através de um programa de mensagens instantâneas tem os mesmos riscos de segurança e de privacidade que o correio electrónico, mas existem alguns perigos particulares que deve conhecer e para os quais deve alertar os seus alunos aquando da utilização desta ferramenta na sala de aula. Durante a preparação e a realização de actividades com recurso às IM, deve ter em atenção que é importante:

- A escolha do nome de ecrã, optando por um que não ponha em evidência as suas informações pessoais.
- Evitar mensagens instantâneas indesejadas, pelo que não se deve indicar o nome de ecrã ou endereço de correio electrónico em áreas públicas (como grandes listas de endereço web, ou perfis de comunidades on-line) nem revelá-lo a estranhos.
- Nunca devemos fornecer informações pessoais, como os números de cartões de crédito ou palavras passe, numa conversa por mensagens instantâneas.
- Tentar comunicar apenas com pessoas que estão na nossa lista de contactos ou de amigos;
- Não aceder encontrarmo-nos pessoalmente com pessoas que só conhecemos através de comunicações por mensagens instantâneas;
- Nunca abrir imagens, transferir ficheiros ou clicar em hiperligações existentes em mensagens de pessoas que não conhecemos.
- Quando não estamos disponíveis para receber mensagens, devemos ter cuidado com a forma como exibimos essa informação, pois podemos não querer que os outros utilizadores saibam onde estamos e a fazer o quê.
- Controlar de perto a utilização de mensagens instantâneas pelos seus alunos, estando sempre próximo deles aquando das actividades de comunicação propostas para a aula;

Usada em segurança, esta ferramenta permite potenciar e desenvolver nos alunos competências diversas como sejam a cooperação e a colaboração na discussão de temas cuja finalidade consiste na realização de um trabalho conjunto. Todavia, para que os dividendos colhidos possam ser potenciados e aproveitados na sua plenitude é necessário ter um cuidado especial na preparação das actividades, de modo a garantir a segurança dos nossos alunos.

### 3.3. Regras de conduta na Internet – evitar situações de conflito

Todos os novos cidadãos da Internet, também chamados *netcitizens*, devem ter presente que existem outros cidadãos e que, tal como na navegação real ou noutra actividade pública, existem regras implícitas de conduta ou etiqueta.

Se não compreendermos como funcionam as regras de cidadania na Internet, isso poderá resultar em muito mais do que a simples perda de uma boa oportunidade. Se dissermos algo errado, na altura errada, isso poderá ser considerado um abuso e provocar outros problemas.

Assim, antes de começarmos a utilizar as ferramentas de comunicação no processo de ensino e aprendizagem, é fundamental saber quais as regras de etiqueta que se usam nestes novos meios de comunicação. Devemos começar por orientar os nossos alunos com **exemplos de boa conduta**, tais como:

- Não escrever com letras maiúsculas – isso significa que ESTÁ A GRITAR;
- Evitar atitudes que possam ser mal interpretadas ou que firam susceptibilidades;
- Evitar utilizar em excesso abreviaturas, pois podem confundir o(s) interlocutor(es);
- Não ofender nem magoar aqueles com quem está a interagir;
- Utilizar uma linguagem própria, adequada e cuidada;
- Utilizar o bom senso;
- Respeitar os outros;
- Tentar escrever mensagens curtas.

Para além da etiqueta e, tendo em conta que, muitas vezes é difícil transmitir emoções ou intenções apenas com o texto, podemos recorrer a símbolos expressivos, ou emoticons. Estes símbolos são expressões faciais virtuais criadas a partir de caracteres do teclado (parênteses, pontos, vírgulas, entre outros) que procuram transmitir as emoções sentidas pelos utilizadores.

Estes são alguns exemplos dos símbolos mais utilizados:

- :-) Feliz ou a brincar
- ;-) A piscar o olho
- :-( Triste
- :-| Ambivalente
- :-o Surpreendido, ou preocupado
- :-x Sem dizer nada
- :-p Com a língua de fora (normalmente a brincar)

Outra ideia que evoluiu para facilitar as comunicações é a utilização de **abreviaturas ou siglas**. Uma vez que podemos falar mais rápido do que escrevemos, é habitual reduzir as frases mais comuns para algumas letras simples. Aqui ficam alguns exemplos das siglas mais utilizadas:

- AFAIK - As Far As I Know (Tanto quanto sei)
- BRB - Be Right Back (Volto já)
- BTW - By The Way (A propósito)
- CU - See you (Até breve)
- FYI - For Your Information (Para sua informação)
- IMHO - In My Humble Opinion (Na minha humilde opinião)
- LOL - Laughing Out Loud (Dar uma gargalhada)
- OAO - Over And Out (Fim de comunicação)
- RUOK - Are You OK? (Está tudo bem?)
- TIA - Thanks in advance (Obrigado antecipadamente)

Estas convenções são o reflexo de normas de bom senso de convivência entre os utilizadores, pelo que é fundamental que os nossos alunos cumpram este conjunto de regras de etiqueta comportamentais. Assim, é necessário, antes de iniciar uma sessão de comunicação on-line, certificarmos de que os alunos compreendem estas regras, bem como verificar, ao longo da sessão, que estas são respeitadas, a fim de evitar situações de risco.

## Ligações Úteis

SeguraNet	<a href="http://www.seguranet.pt/">http://www.seguranet.pt/</a>
Internet Segura	<a href="http://www.internetsegura.pt/">http://www.internetsegura.pt/</a>
Sítio dos Miúdos – Página para pais e professores	<a href="http://www.sitiodosmiudos.pt/paiseducadores/">http://www.sitiodosmiudos.pt/paiseducadores/</a>
Junior – Pais e Educadores	<a href="http://www.junior.te.pt/servlets/Gerais?P=Pais&amp;ID=1130">http://www.junior.te.pt/servlets/Gerais?P=Pais&amp;ID=1130</a>
SafeKids	<a href="http://www.safekids.com/welcome.htm">http://www.safekids.com/welcome.htm</a>
GetNetWise	<a href="http://www.getnetwise.org/">http://www.getnetwise.org/</a>
Safe Use of the Internet	<a href="http://www.netaware.org/gb/website.html">http://www.netaware.org/gb/website.html</a>
Be Safe Online	<a href="http://www.besafeonline.org">http://www.besafeonline.org</a>
The Urban Legends Reference Pages	<a href="http://www.snopes.com/">http://www.snopes.com/</a>

### **Nós Europeus InSafe**

Áustria	<a href="http://www.saferinternet.at/">http://www.saferinternet.at/</a>
Espanha	<a href="http://www.protegeles.com/">http://www.protegeles.com/</a>
UK	<a href="http://www.uclan.ac.uk/host/cru/">http://www.uclan.ac.uk/host/cru/</a>
Bélgica	<a href="http://www.saferinternet.be/">http://www.saferinternet.be/</a>
Holanda	<a href="http://www.digibewust.nl/">http://www.digibewust.nl/</a>
Alemanha	<a href="http://www.klicksafe.de/">http://www.klicksafe.de/</a>
Itália	<a href="http://www.saferinternetday.it/">http://www.saferinternetday.it/</a>
Polónia	<a href="http://www.saferinternetday.pl/">http://www.saferinternetday.pl/</a>
Hungria	<a href="http://www.baratsagosinternet.hu/mss/alpha">http://www.baratsagosinternet.hu/mss/alpha</a>
Dinamarca	<a href="http://andk.medieraadet.dk/">http://andk.medieraadet.dk/</a>
Finlândia	<a href="http://www.tiukula.fi/index.php">http://www.tiukula.fi/index.php</a>
Grécia	<a href="http://www.saferinternet.gr/">http://www.saferinternet.gr/</a>
Islândia	<a href="http://www.heimiliogskoli.is/">http://www.heimiliogskoli.is/</a>
Irlanda	<a href="http://www.ncte.ie/InternetSafety/">http://www.ncte.ie/InternetSafety/</a>
Lituânia	<a href="http://www.bite.lt/en/">http://www.bite.lt/en/</a>
Noruega	<a href="http://www.saftonline.no/">http://www.saftonline.no/</a>
Eslovénia	<a href="http://www.safe.si/">http://www.safe.si/</a>
Suécia	<a href="http://www.medieradet.se/">http://www.medieradet.se/</a>