FUNDAÇÃO

COMUNICAR EM SEGURANÇA

Guião do Formador

Secundário

BREVE NOTA

O programa **"Comunicar em Segurança"** teve início em 2009 e o ano letivo 2015/2016 será a **7ºedição** do programa. Em 6 anos, o programa já chegou a mais de 266 mil alunos e 1.853 escolas com mais de 8.000 sessões de sensibilização realizadas por mais de 500 voluntários.

Através das sessões em contexto escolar, o objetivo é transmitir aos alunos do ensino secundário noções básicas de segurança na Internet. Com esta iniciativa, PT , PSP e ANPRI – Associação Nacional de Professores de Informática contribuem para a redução dos perigos que o uso desadequado da internet pode representar, sobretudo, junto dos mais jovens.

O presente **Guião** constitui um guia para a apresentação, exposição e discussão dos conteúdos no âmbito da comunicação através das novas tecnologias, em particular através da INTERNET e visa apresentar instrumentos e orientações técnicas para o bom desempenho do polícia/voluntário afeto às sessões do "**Comunicar em Segurança- Secundário**".

1. OBJETIVO DA AÇÃO

Transmitir os conhecimentos necessários de forma a prevenir e a reagir contra os riscos *online* a que estão sujeitas as crianças.

2. METODOLOGIA DA AÇÃO

Pretende-se que os **conteúdos sejam transmitidos com um caráter de envolvimento dos alunos e professores.**

3. ITINERÁRIO PEDAGÓGICO

O **Comunicar em Segurança 2015/16** para o secundário aborda os temas: **Password, privacidade e partilha de informação pessoal na Internet, *cyberbullying e* segurança móvel**.

A forma mais adequada de iniciar a sessão é explicar em que consiste o **Comunicar em Segurança,** um projeto da **Fundação Portugal Telecom (Fundação PT)** em parceria com a **PSP (Polícia de Segurança Pública) / ANPRI**, que pretende transmitir boas práticas para o uso correto e seguro da internet e telemóveis.

É importante explicar aos alunos o motivo pelo qual a PT , a PSP e ANPRI estão juntas neste programa: A PT, enquanto empresa que fornece Internet e telemóveis, pretende que as crianças e jovens usem a Tecnologia de uma forma segura e consciente, e é necessário terem alguns cuidados para estarem seguros no dia-a-dia. Se as crianças não tiverem alguns cuidados, colocam a sua segurança física em risco, sendo esta uma das grandes preocupações da PSP/dos professores.

Durante a apresentação, passe os slides e deixe que sejam os alunos a dizer qual a resposta certa e porquê. Incentive-os os sempre a justificarem as opções de modo a que sejam os alunos a chegar à resposta correta. Existem slides informativos que sintetizam as boas práticas que os alunos devem seguir.

4. SLIDE 1

Comece por apresentar-se e informar que trabalha na PT (Portugal Telecom) / PSP (Policia de Intervenção Pública) e que irá falar com a turma sobre Internet e telemóveis e que cuidados devem ter quando navegam na Internet.

Sendo professor de Informática, a apresentação será, necessariamente, diferente, uma vez que a sessão será realizada em contexto de aula.

5. SLIDE 2

O **Slide 2** é o início da apresentação e funciona como um quebra-gelo.

Explique à turma que a Internet é fantástica e que, de facto, parece difícil pensarmos viver sem Internet ou telemóvel. Fazemos muitas coisas na Internet, como pesquisas para os trabalhos da escola, falar com os primos, amigos ou pais que estão longe, ouvir música, jogar, etc.

Sem darmos conta, quando utilizamos a Internet e navegamos horas infinitas, não nos apercebemos como estamos a deixar a nossa "pegada digital". Pergunte à turma se sabem o que é a nossa "Pegada Digital"?

Informe-os que tudo fica registado na Internet, pelo que devem pensar bem antes de colocar informação online. Tudo o que se coloca na Internet permanece online e torna-se a nossa pegada digital que poderá ser vista por qualquer pessoa.

Alerte-os que o que colocam hoje na Internet, pode ser visto daqui a 5 ou 10 anos.

As imagens que surgem na apresentação são um bom exemplo que as pessoas estão a colocar tanta informação online, que é sempre possível seguir os passos de uma pessoa.

6. SLIDES 3 A 5 (PASSWORD)

A apresentação começa com o tema da password. No **slide 3**, pergunte à turma o que têm de escrever quando querem aceder ao email, ao jogo, ao facebook? Após as respostas da turma, revele o símbolo da password e diga-lhe que devem reter esta imagem. Diga aos alunos que a password é como se fosse a chave de casa. Pergunte-lhes se eles dão a chave de casa a alguém, ao melhor amigo? A resposta imediata será não, e nesse sentido, também não deverão partilhar a password com ninguém. A password é pessoal e confidencial.

A outra comparação que deve passar aos alunos é da escova de dentes, que não se partilha com ninguém.

Avise a turma que a password não se partilha com as melhores amigas ou futuros namorados, uma vez que se se chatearem, as amigas podem entrar nas contas de e-mail ou facebook e enviar mensagens falsas.

Informe os alunos que uma password segura é muito importante para navegarem em segurança na Internet, uma vez que uma má password facilita o acesso aos computadores onde, em muitos casos, estão informações pessoais (por exemplo fotos, emails, etc).

Leve-os a pensar que utilizamos palavras-chave em muitas situações na nossa vida, e que por esse motivo, é importante termos palavras-chave difíceis. Pode utilizar o exemplo do código de multibanco, que também é uma password. Pode contar-lhes uma história verdadeira que foi partilhada por um polícia – *Um senhor perdeu a*

carteira, onde tinha o cartão multibanco e ao lado o cartão de cidadão. A pessoa que encontrou a carteira em vez de ir à esquadra entregar a carteira, foi ao multibanco. Lembrem-se que na carteira, ao lado um do outro estavam o cartão multibanco e o cartão de cidadão. Pergunte à turma: *Imaginam/Sabem que código o ladrão colocou para roubar o dinheiro?* O código foi o ano de nascimento que estava no cartão de cidadão.

Este é apenas um exemplo, para as crianças entenderem que não utilizamos só palavras – chave no computador, e que a password é um código secreto, e devemos ter códigos difíceis das outras pessoas descobrirem.

Antes de revelar como se cria uma password segura, pergunte à turma quem acha que tem uma password má. É normal que poucos alunos levantem os dedos.

Após ter as respostas dos alunos, revele as "regras" para criar uma password segura **(Slide 4).** Depois de todos verem o slide, questione novamente a turma:

1. Quem tem passwords só com letras?
2. Quem tem passwords com letras e números?
3. Quem tem passwords com letras, números e caracteres especiais?

Com este pequeno jogo, irá perceber que poucos alunos têm passwords complexas. De seguida poderá informar a turma que passwords de letras demoram segundos a descobrir; passwords com letras e números levam minutos ou poucas horas, mas que passwords com letras, números, caracteres especiais, maiúsculas e minúsculas são muito difíceis de descobrir, e que quem tenta aceder aos computadores e contas pessoais, acede aos que são de entrada imediata.

Posteriormente, diga aos alunos que vai ensinar algumas técnicas para terem passwords mais seguras. No **slide 6** estão várias sugestões de como podem ter uma password segura utilizando símbolos especiais; frase mistério e passwords diferentes para vários acessos.

Algumas dicas sobre segurança de passwords que deve transmitir aos alunos:

1. Explique-lhes que os dados pessoais, como por exemplo o nome deles, dos pais, irmãos, nomes dos animais, datas de nascimento, nome da escola ou rua, são um alvo fácil de descobrir e que serão as primeiras tentativas que alguém vai fazer para tentar aceder ao computador ou às páginas pessoais.
2. Deve informar os alunos que a password é pessoal e confidencial e que por esse motivo não deve ser partilhada com ninguém.
3. Alerte-os que não devem escrever a palavra-chave em papeis, ficheiros ou contatos de telemóvel, pois caso percam a carteira ou o telemóvel, outras pessoas podem descobrir a password. A password tem que estar na memória.
4. Incentive os alunos a alterarem a password com frequência e a não escolherem a opção de "guardar password", pois caso alguém aceda ao computador pessoal, e as passwords estiverem todas memorizadas, facilmente acedem a aplicações e informações que são de acesso restrito.
5. Por fim, informe os alunos que devem ter várias passwords para vários serviços, porque no caso de falhar a segurança de uma, não falha das outras.

7. SLIDES 6 A 11 (PRIVACIDADE E PARTILHA DE INFORMAÇÃO PESSOAL)

Um dos maiores erros que as crianças e jovens fazem é partilhar demasiada informação pessoal na Internet, sem se aperceberem que no mundo virtual podemos ser quem não somos, e que os amigos virtuais podem não ser aquilo que dizem ser.

Nesse sentido, há que prevenir estes comportamentos e as crianças perceberem que no mundo virtual devem ter os mesmos cuidados que têm no dia-a-dia.

No **slide 6** estão várias perguntas que deve colocar à turma e ver as respostas. São perguntas cuja resposta é NÃO. Depois das respostas da turma, faça nova pergunta: e na Internet, o que fazem?

Depois de lançar a pergunta, informe a turma que vão ver um vídeo.

Passe o vídeo (**slide 7**) e pergunte aos alunos se perceberam o filme e se entenderam quais os riscos associados à partilha excessiva de dados pessoais.

No **slide 8** deve informar a turma sobre os cuidados que devem ter na Internet e recordá-los que todos os cuidados que têm no dia-a-dia, devem ter na Internet, como por exemplo não falar com pessoas que não conhecem, não aceitar pedidos de amizade de desconhecidos; confirmar os pedidos de amizade de "amigos" porque todos podemos criar perfis falsos e a Joana da escola pode ser afinal outra pessoa. Ensine-os a fazer uma pesquisa do nome da pessoa. Se encontrarem 2 nomes iguais com a mesma fotografia, é porque um dos perfis é falso. Peça aos alunos para ligarem aos amigos a confirmarem o pedido de amizade.

Informe a turma que se **o Facebook fosse um país, seria o 3 maior país do Mundo**, e que existem cerca de **80 milhões de perfis falsos**.

Informe-os que não devem colocar online ou dizer onde moram, a escola onde andam, os nrºs de telefone ou telemóvel, os passatempos.

Alerte-os para a questão das fotografias que colocam nas Redes Sociais. Informe-os que uma vez na Internet, para sempre na Internet e que tudo o que está na Internet pode ser visto por outras pessoas que não conhecem e que as fotografias podem ser modificadas e utilizadas para outros fins. Explique aos alunos que por vezes o cenário das fotografias é mais importante que a imagens deles, pois pode revelar estilos de vida, onde moram, estudam, passam férias, etc.

Explique aos alunos que todas as fotos, vídeos e mensagens que sejam colocadas na Internet, sem nenhum tipo de restrição, ficam acessíveis para todos verem.

Informe-os que nas Redes Sociais existem **Políticas de Privacidade** e que podem, por exemplo, mostrar as fotos só a alguns amigos e familiares e não a todos os amigos que têm na rede social. Pode informá-los que as **Políticas de Privacidade** podem ser consultadas e modificadas nas **Definições da Conta** e que se precisarem de ajuda, devem falar com os pais, irmãos ou professores. Explique às crianças que existe uma opção muito importante – a opção **Restrito**. Quando aceitam uma pessoa como amiga, mas colocam essa pessoa como **Restrito**, essa pessoa apenas vê a fotografia do perfil, mas eles conseguem ver tudo do perfil dessa pessoa.

Saliente que a imagem deles é muito importante e que não deve ser partilhado com todas as pessoas. Utilize o exemplo da declaração dos pais que autorizam ou não que a escola divulgue a imagem dos filhos na Internet. Por exemplo, se existir uma gravação

de uma estação de televisão, a escola tem sempre de pedir autorização aos pais para os filhos aparecerem na televisão. A imagem é um bem, um direito.

Pode também informar a turma que não adianta ter muitos amigos nas redes sociais se não os conhecerem na realidade; deixe-os pensar se as fotos que já têm publicadas estão protegidas ou visíveis para todas as pessoas e os riscos que podem ter; Informe-os que, por definição, toda a informação que se introduz está disponível para todas as pessoas. É necessário restringir a informação disponível, para que as pessoas que não conhecemos consigam apenas ver o nosso nome (por exemplo). Mesmo quando já são nossas amigas, podemos restringir as nossas fotografias, para que só os pais e família as vejam.

Informe-os que se tiverem um perfil nas redes sociais, este deve ser privado e não devem partilhar informação pessoal para que pessoas desconhecidas não tenham acesso a informação confidencial. Para criar o perfil privado, têm de ir às **Definições de Conta** e **Definições de Privacidade.**

Muitas vezes, os alunos colocam fotografias que permitem a sua localização, como por exemplo fotografias com o nome da escola, fotografias que identificam o local de residência ou os locais onde praticam tempos livres.

É muito importante que transmita a ideia que não coloquem fotografias que permitam a localização. Pode recorrer ao exemplo do Gang mexicano que escolhia as vitimas através da informação que as pessoas nas redes sociais. Através das fotografias, conseguiam ver se as pessoas tinham boas condições financeiras, quais os seus hábitos de vida, os seus amigos e familiares e de uma forma simples, planeavam o sequestro, com base na informação encontrada na Internet.

Por exemplo, no Facebook existe a possibilidade de colocar a localização através do telemóvel, nada melhor para encontrar alguém ou saber que a pessoa não está em casa. Incentive os alunos a serem os professores dos pais e explicarem-lhes que não devem escolher esta opção/aplicação Check-In, para que nunca se saiba onde estão.

A fotografia do **Slide 9** é um bom exemplo do tipo de fotografias que as pessoas partilham, ignorando que estão a colocar online informação pessoal.

No **Slide 10** está o exemplo de Paris Brown, que aos 16 anos, foi 1ª Jovem britânica a ser eleita para o cargo '*Youth Police Crime Commissioner*'. No entanto, resigna antes de ocupar o lugar, por pressão dos media devido aos comentários homofóbicos, racistas e sobre o uso de drogas da sua conta de twitter, 2 anos antes.

Relembre a turma que uma vez na Internet, para sempre na Internet, e que devem ter cuidado com as fotografias e comentários para estes não serem prejudiciais no futuro.

8. SLIDES 12 E 13 (CYBERBULLYING)

Antes de revelar a informação do **slide 12**, e iniciar o tema do *cyberbuulying*, pergunte à turma "**Sabem o que é *bullying*?**"

Após a turma responder, informe que ***bullying* é:**

1. Uma agressão que pode ser física, verbal, emocional, psicológica
2. Intencional, repetida e continuada
3. Feita por uma pessoa ou por um grupo de colegas sempre dirigida ao mesmo colega/pessoa.

Após dar esta definição, pergunte à turma: "**Gostam de ser gozados, ofendidos, mal tratados?".** A resposta será não. De seguida, diga: *Então se não gostam, não façam aos outros. Se não gostam de ser gozados, não gozem com os vossos colegas.*

Informe a turma que está nas mãos deles acabarem com o *Bullying e Cyberbullying* nas escolas, porque é seguir o velho ditado popular – "***Não faças aos outros, aquilo que não gostas que te façam a ti!"***

Peça aos alunos para pensarem um pouco nos outros, e antes de fazerem, pensarem se gostavam de estar naquela situação.

Informe as crianças que devem sempre pedir ajuda a pessoas mas velhas, pais ou professores, e que não devem acreditar quando o agressor diz: " *Se contares, vai ser pior"*. Os agressores querem o medo das vítimas, mas se as vítimas pedirem ajuda e falarem com os professores, são todos chamadas à responsabilidade - agressor, vitima, pais do agressor/vítima e a polícia (se assim pretenderem)

No entanto, por vezes é difícil das crianças vítimas terem coragem. Assim, peça aos colegas para terem a coragem que falta a esse menino/a, e para serem eles a contar ao professor ou aos pais. Explique-lhes que não estão a ser "queixinhas", mas sim corajosos. Relembre-os que hoje não é com eles, mas que amanhã poderá ser. Hoje são os valentes, os heróis da escola/da turma, para o ano vão para outra escola onde já existem outros mais velhos.

Após falarem de *bullying*, pergunte á turma o que é o *cyberbullying*. No **slide 13,** questione a turma se sabem o que significa a palavra *Cyberbullying* . Após as suas respostas, apresente o slide, explicando que o *cyberbullying* é uma palavra que deriva de *bullying* e conforme o *bullying* também é uma agressão praticada através da Internet e dos Telemóveis. Os agressores ofendem e agridem as vítimas, recorrendo aos *emails,* ao chat, às redes sociais, blogs e mensagens de telemóvel, mantendo-se assim no anonimato. Explique-lhes que *cyberbullying* é alguém fazer um vídeo de um colega e colocá-lo na Internet. Pergunte quem é pior:

1. Quem faz o filme e coloca na Internet?
2. Quem faz Gosto?
3. Quem partilha?
4. Quem comenta?

É norma ter várias opiniões. No final, em tom de questão, diga – "*E não são todos? Não será tão mau aquele que coloca o filme na Internet como aquele que faz gosto e partilha o vídeo?* Diga-lhes para acabarem com este tipo de situações, que está nas mãos deles.

Questione a turma sobre o que devem fazer se forem vítimas de *cyberbullying* e após as respostas, revele as opções. É importante que transmita aos alunos que devem sempre reportar o abuso, porque se não contarem a ninguém, ninguém poderá ajudar. Em situações de *cyberbullying* é importante que as mensagens de telemóvel, chats ou emails sejam gravados pois podem servir de prova contra o agressor. Por outro lado, as vítimas não devem responder ao agressor, porque muitas vezes é isto que o agressor pretende, e respondendo ao agressor estão a descer ao mesmo nível dele.

Alerte-os para o fato que as fotografias partilhadas na Internet e informação pessoal, podem ser aproveitadas para situações de *cyberbullying* e por mais este motivo, devem ter todo o cuidado ao colocarem fotos na Internet.

9. SLIDES 14 (SEGURANÇA NOS TELEMOVEIS)

O **Slide 14** aborda o tema da segurança no telemóvel.

Informe os alunos que, atualmente, os telemóveis são pequenos computadores e nesse sentido, devem ter os mesmos cuidados que têm no computador.

No **slide 14** estão algumas mensagens que deve transmitir, nomeadamente, questões relacionadas com fotos tiradas no telemóvel que depois são colocadas na Internet e que têm localização; alerte-os que fotos que são tiradas com Iphone estão sempre na Internet, porque automaticamente estão guardadas na *cloud* da Apple; ter atenção á

informação pessoal que se guarda nos telemóveis e que facilmente pode ficar acessível a pessoas desconhecidas ou mesmo conhecidas no caso de não termos um pin seguro de bloqueio do telemóvel.

Outra questão relacionada com a segurança móvel é as APPS. Alerte os alunos para terem atenção que informação fica disponível/acessível ao fornecedor da APP quando instalam uma APP no telemóvel. Quase todas as APPS pedem acesso á agenda e imagens. Será que queremos que empresas fiquem com acesso às nossas fotos?

Após passar estes conselhos, mostre 2 aplicações semelhantes para a turma verificar que sendo semelhantes, são bastante diferentes uma vez que uma delas pede acesso a informação pessoal. A escola é do utilizador.

10. SLIDES 15 A18 (ESQUEMAS DE FRAUDE)

A apresentação termina com os esquemas de fraude. **No slide 15** poderá explicar à turma que tipos de fraude existem no mundo virtual: ***phishing e spam.***

Pode informar os alunos que tanto o *phishing* como o *spam* são esquemas de fraude realizados na Internet, efetuados por profissionais com o objetivo de enganar as pessoas.

Os **slides 16 e 17** são casos reais de *phishing*, nos quais existiu o aproveitamento de entidades credíveis e reconhecidas para serem cometidos os crimes.

No **slide 18** estão algumas mensagens que deverá transmitir de modo aos alunos estarem mais alerta com este tipo de fraude:

1. Não fazer o download ou instalar os programas que aparecem no computador, sem terem pedido. Em muitos casos, ao fazer-se o download do programa

estamos a instalar um programa de vírus no computador, que pode copiar toda a informação que têm no computador, desde as passwords até ás fotos e vídeos.

2. Alerte-os para os *links* enviados por emails, pois podem ser também uma forma de *phishing* ou vírus. Informe-os que nunca devem carregar nos *link*s. Se quiserem aceder à página, devem escrever o endereço na barra do Internet Explorer e ver para onde são encaminhados. Em muitos casos, as páginas/sites parecem ser verdadeiros, mas são um espelho que pretendem obter os dados pessoais.
3. Não confirmar os dados pessoais. Se algum *email* pedir a confirmação de dados pessoais (*password*, nome, morada, telefone), nunca devem responder. Aconselhe-os a dizerem aos pais que, se tiverem *homebanking* (acederem à conta do banco no computador) deverão ter um cuidado redobrado porque uma grande maioria destes esquemas de fraude acontecem com e-mails que as pessoas pensam que foram mesmo enviados pelo banco.
4. Ter atenção a *emails* muito aliciantes, sugestivos, ou/e de remetentes omissos.

Observação:

Comunique aos alunos e professor que poderão participar no Passatempo Comunicar em Segurança. Podem encontrar o regulamento no site http://comunicaremseguranca.sapo.pt