FUNDAÇÃO

COMUNICAR EM SEGURANÇA

Guião do Formador

Seniores

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.

Nestes 6 anos o programa teve como público-alvos jovens e educadores, mas uma vez que a Internet é utilizada por toda a comunidade, e a população sénior tem um contacto cada vez maior com as Novas Tecnologias e existindo ainda um desconhecimento grande perante as Novas Tecnologias, o ano 2015/2016 marcará o início de sessões de Comunicar em Segurança para Seniores.

Com esta iniciativa, a PT, a PSP e ANPRI - Associação Nacional de Professores de Informática contribuem para a redução dos perigos que o uso desadequado da internet pode representar junto da população sénior.

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-Séniores**".

1. Objetivo da ação

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

2. Metodologia da ação

Pretende-se que os **conteúdos sejam transmitidos com um caráter de envolvimento do público/formador.**

3. Itinerário pedagógico

O **Comunicar em Segurança 2015/16 - Seniores** aborda os temas: **Password, privacidade e partilha de informação pessoal na Internet, *cyberbullying* , *esquemas de fraude 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)**, que pretende transmitir boas práticas para o uso correto e seguro da internet e telemóveis.

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

4. SLIDE 2

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

5. SLIDE 3

O **Slide 3** é o início da apresentação.

Explique ao grupo 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.

No entanto, existem também alguns riscos associados às Novas tecnologias tal como os esquemas de fraude, falta de privacidade, ou stalking.

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

Informe 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.

6. SLIDES 4 A 6 (PASSWORD)

A apresentação começa com o tema da password. No **slide 4**, pergunte ao grupo o que têm de escrever quando querem aceder ao email, ao jogo, ao facebook? Após as respostas do grupo, revele o símbolo da password e diga-lhe que devem reter esta imagem. Diga ao grupo que a password é como se fosse a chave de casa. Pergunte-lhes se eles dão a chave de casa a alguém? 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 pode passar aos alunos é da escova de dentes, que não se partilha com ninguém.

Informe o grupo 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 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 ao grupo quem acha que tem uma password má. É normal que poucas pessoas levantem os dedos.

Após ter as respostas, revele as "regras" para criar uma password segura **(Slide 5).** Depois de todos verem o slide, questione novamente:

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 poucas pessoas 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, informe o grupo 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:

1. Explique-lhes que os dados pessoais, como por exemplo o nome deles, dos filhos netos, nomes dos animais, datas de nascimento, nome da 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 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 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 que devem ter várias passwords para vários serviços, porque no caso de falhar a segurança de uma, não falha das outras

7. SLIDES 7 A 10 (PRIVACIDADE E PARTILHA DE INFORMAÇÃO PESSOAL)

Um dos maiores erros que as pessoas 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 pessoas perceberem que no mundo virtual devem ter os mesmos cuidados que têm no dia-a-dia.

No **slide 7** estão vários cuidados a ter na Internet:

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. 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.

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, o trabalho dos filhos/netos, escolas dos netos, os nrºs de telefone ou telemóvel.

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 ao grupo que por vezes o cenário das fotografias é mais importante que a imagens deles, pois pode revelar estilos de vida, onde moram, passam férias, etc.

Explique 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**. Explique ao grupo 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.

Pode também informar 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 algumas pessoas 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.** Pode utilizar o vídeo do Tutorial do Facebook para este efeito.

Muitas vezes, as pessoas colocam fotografias que permitem a sua localização, como por exemplo 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 8** é um bom exemplo do tipo de fotografias que as pessoas partilham, ignorando que estão a colocar online informação pessoal.

No **Slide 9** está o exemplo de uma modelo belga que perdeu um contrato com a Loreal devido à fotografia e comentários que tinha na sua página de Facebook sobre caça.

Relembre o grupo que uma vez na Internet, para sempre na Internet.

8. SLIDES 11 A15 (ESQUEMAS DE FRAUDE)

No slide 11 poderá explicar ao grupo que tipos de fraude existem no mundo virtual: ***phishing e spam.***

Pode informar 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 13 e 14** são casos reais de *phishing*, nos quais existiu o aproveitamento de entidades credíveis e reconhecidas para serem cometidos os crimes.

No **slide 15** estão algumas mensagens que deverá transmitir de modo ao grupo estar 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 *phishin*g 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.

9. SLIDES 16 AO 19 (SEGURANÇA NOS TELEMOVEIS)

O **Slide 16** aborda o tema da segurança no telemóvel.

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

No **slide 16** 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 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?

Os **slides 17 e 18** são dados estatísticos interessantes sobre os dados que ficam acessíveis para os fornecedores das aplicações.

Após passar estes conselhos, no **slide 19** 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.