Gestão de Identidade

I – Alfabeto Secreto

Proposta de Jogo Didáctico para Sensibilização sobre Segurança

Esta actividade tem como objectivo sensibilizar as crianças (11-12 anos) para alguns aspectos da segurança, nomeadamente como garantir a confidencialidade da informação trocada em ambientes potencialmente hostis, tais como redes sociais, emails, forae, chats, etc...

A actividade é para ser realizada em grupo, numa aula, ou atelier de tempos livres.

A Ana e o Bruno são amigos e gostam de trocar mensagens sem que ninguém presente na sala possa perceber o que estão a dizer um ao outro.

Para isso, combinam entre si uma forma de escrever mensagens que ninguém mais possa perceber: escrevem tudo num **alfabeto secreto** que torna o texto incompreensível para quem não conheça o **segredo**.

Assim, Ana e Bruno encontram-se num local onde não haja ninguém por perto, e combinam o seguinte segredo:

"Em vez de escrever as palavras normalmente, vamos utilizar um código secreto! Vamos trocar cada letra da mensagem por uma outra, deslocando o alfabeto um certo número de posições para a direita".

Como indicado neste exemplo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Neste caso, o segredo combinado entre Ana e Bruno foi o número 3, já que o alfabeto secreto corresponde a uma deslocação de 3 posições para a direita do alfabeto original. Esta operação designa-se por encriptação.

Assim por exemplo, as palavras (texto em claro):

"**alfabeto secreto**"

transformam-se em (texto encriptado):

"**doidehwr vhfuhwr**".

Para voltar ao texto original, faz-se a operação inversa, ou seja, desloca-se cada letra do texto secreto 3 posições para a esquerda: o "d" dá um "a", o "o" dá um "l", e assim de seguida. Esta operação designa-se por desencriptação.

O mais engraçado, é que a Ana e o Bruno podem combinar um segredo diferente para cada dia da semana, por exemplo na 2ª feira é 2, na 3ª 3, na 4ª 4 na 5ª 5 e na 6ª 6, ou outros quaisquer que queiram imaginar, desde que sejam compreendidos entre 1 e 25. Têm assim 25 segredos diferentes que podem utilizar.

No decorrer da actividade, os alunos poderão formar grupos de 2, escolhendo um colega com o qual irão trocar mensagens (Ana e Bruno).

A actividade poderá ter o seguinte encadeamento:

1. Ana e Bruno combinam o segredo que irão utilizar, que mais ninguém deve conhecer, devendo para isso sair da sala por breves instantes.
2. A Ana encripta uma mensagem secreta para o seu correspondente.
3. A Ana envia a mensagem a Bruno, fazendo-a passar pelos seus colegas, que a podem ler, sem obviamente entender o seu significado.
4. Bruno recebe a mensagem secreta e utilizando o segredo que combinou com a Ana, desencripta o seu conteúdo.
5. Bruno responde a Ana utilizando o mesmo alfabeto secreto.
6. Etc...

Para ajudar na escrita das mensagens secretas, os alunos poderão utilizar pequenas aplicações on-line, como por exemplo:

http://cryptoclub.org/tools/caesar_cipher.php

http://inventwithpython.com/cipherwheel/

Para perceber até que ponto esta forma de trocar mensagens secretas é válida, a actividade prossegue depois com exploração do Problema do Segredo.

Para Ana e Bruno combinarem um segredo que mais ninguém conheça, tiveram de sair da sala por momentos. E o que acontece se Ana e Bruno não puderem sair da sala? Como vão poder trocar o segredo?

O resto da sessão poderá ser preenchido com os alunos a tentar imaginar soluções para este problema.

A descoberta de uma possível solução poderá ser objecto de uma outra actividade: **Partilha de Segredo**.