



# Internet Mais Segura

Turma Redes 18 - 2021



**Safer  
Internet  
Day 2021** | Tuesday  
9<sup>th</sup> February


**Together for a better internet**

# News...

## Rapper Pop Smoke assassinado em casa. Músico vinha este ano ao festival Rolling Loud no Algarve

O rapper terá sido assassinado na casa onde se encontrava em Los Angeles, avançam vários meios de comunicação americanos.

SHOW MAG  
19 FEV 2020 15:44  
SHOWBIZ



8 julho 2019 21:04  
Suspeito de homicídio do rapper Nipsey Hussle foi preso

8 maio 2019 09:35  
'Shalker' é preso por invadir casa de Taylor Swift pela segunda vez

DESCUBRA A GAMA 500X  
DESDE 160€/MÊS  
TAEG 8,0%

SAIBA MAIS

SAPO VOUCHER

CRUZEIRO GOLFINHOS  
DESDE 17,50€

## Google descobre grave falha de segurança no iPhone

Ataque fornece acesso a conversas em mensageiros e dados pessoais. Vulnerabilidades foram corrigidas pela Apple no início do ano

Por Marvin Costa, para o TechTudo

31/08/2019 08h08 · Atualizado há 5 meses



# Dia Internet mais Segura



O Dia da Internet Mais Segura tem como objetivo promover a utilização consciente e responsável, crítica e criativa das tecnologias, especialmente entre as crianças e os jovens, e sensibilizar todos os stakeholders a desempenharem o seu papel para a criação de uma Internet melhor.

# Ameaças na Internet

- Malware
- Spyware
- Adware
- Cavalos de Tróia
- Ransomware
- Phishing
- Hacking



# Pornografia

- O grande problema de assistir a pornografia é pela existência de vírus em imensos sites pornográficos.



# Jogos online

- Não há legislação adequada e específica para o efeito;
- Siga uma contabilidade muito rigorosa das suas apostas;
- Não utilize cartões de crédito;
- Estabeleça um limite de tempo para jogar.



# P2P

- São sistemas que permitem a partilha de ficheiros entre utilizadores de forma direta
- Problemas:
  - Violação dos direitos de autor;
  - Propagação de malware;
  - Ficheiros falsos.



# Cyberbullying

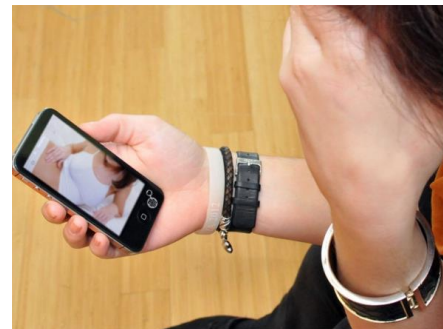
- O termo “Cyberbullying” corresponde às práticas de agressão moral organizadas por grupos, contra uma determinada pessoa e alimentadas via internet
- Motivações:
  - Roubo de identidade;
  - Humilhação pública;
  - Envio de malware;
  - Ameaça e perseguição.





# Sexting

- Sexting refere-se a divulgação de conteúdos eróticos e sensuais através de telemóveis.
- Traduz-se em mensagens SMS, envio de fotografias e vídeos em posições sensuais ou nus, selfie ("selfie de nudez") ou simplesmente nude
- Motivações:
  - Solicitação do parceiro(a) para fazê-lo sob chantagem emocional;
  - Ser convencido por alguém a fazê-lo durante uma conversa online;
  - Envio por vingança de fotos ou mensagens de terceiros.



# Quer mesmo partilhar essa foto

Em redes sociais como o Facebook ou o Instagram, é normal ceder à tentação de, por vezes, partilhar fotografias pessoais.

Nada contra: certifique-se, porém, que só a sua rede de amigos é que pode ver o que partilha. Porque nunca se sabe quem é que está do outro lado...



# Redes Sociais

- Muito tempo online afeta a saúde mental e física.
- Não acreditar em tudo o que vê.
- Não publicar fotos de família com dados.
- Não falar com desconhecidos.
- Usar perfil privado.
- Ser seletivo na escolha de amizades.
- Roubo de identidade: pessoas que fazem ações maléficas em nome de identidades roubadas com consequências nefastas para os verdadeiros portadores dessa identidade.



# Autenticação de dois passos

Sempre que possível, ative a autenticação de dois passos das plataformas online onde está registado(a). Isto torna muito mais difícil que alguém pirateie a sua conta, já que deixa de bastar uma password para entrar com o seu registo: passa a ser necessário, também, inserir um código numérico ou alfanumérico recebido por SMS/email ou gerado por uma aplicação externa geradora de códigos.



# RATs - Remote Access Trojans

Os hackers são capazes de obter acesso aos computadores das vítimas usando RATs (Remote Access Trojans), um tipo de malware que fornece acesso remoto ao computador através de sua conexão com a Internet. Alguns tipos de RAT incluem uma função que permite o acesso à webcam de quem foi infectado sem o seu conhecimento.



# Navegação anónima

O que é?

É uma janela do navegador que não regista informações, como nomes de utilizador e passwords.

Quando uso?

Quando estamos a utilizar um computador de outra pessoa ou de um espaço público.



CTRL + SHIFT + N



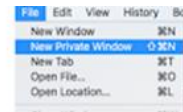
CTRL + SHIFT + P



CTRL + SHIFT + P



CTRL + SHIFT + N



# Ligação Segura



Endereço com “https” em vez do normal “http”, quando se utiliza uma ligação segura.



Cadeado de cifragem: símbolo que indica que é seguro revelar os dados pessoais a um sítio na Rede.

# Como navegar de forma segura



- Utilizar senhas diferenciadas para os vários serviços;
- Não disponibilize informação privada inadvertidamente;
- Não partilhe informação pessoal ou íntima;
- Não forneça a sua palavra-passe a ninguém;
- Guarde registos de todas as mensagens que recebe;
- Não aceite pedidos de amizade de um perfil com conteúdos inapropriados  
'ou que o deixe desconfortável.



# Proteção de Equipamentos



- Manter sempre os sistemas atualizados
- Proteger o telemóvel / PC com uma password forte
- Ativar o bloqueio quando o aparelho estiver inativo
- Não instalar programas de terceiros
- Para evitar surgir algum tipo de vírus no computador, a solução é ter um antivírus pago
- Cuidados com redes públicas:
  - Ser cauteloso no acesso a redes Wi-Fi abertas
  - Não aceder a páginas que contenham informação pessoal
  - Não aceder às contas pessoais

# O aluno Imprudente Caetano

Segundo um recente estudo da Google, 8,7% dos portugueses já foi vítima de fraude online. E à medida que se torna mais fácil e constante o acesso à Internet esses números terão tendência para aumentar. Mas tal como uma condução defensiva minimiza riscos na estrada, também uma navegação defensiva tem o mesmo efeito na Internet.

**Queres juntar-te aos 8,7% dos portugueses atacados  
?**

# Como o Imprudente Caetano circula na internet?

Mantenha o software sempre desatualizado;

Use passwords simples;

Disponibilize dados pessoais;

Partilhe todas as fotos;

De onde é que conhece esse novo amigo?

Pagar contas? Em qualquer lugar;

Não ative as autenticações de dois-passos;

Aceite pedidos de estranhos;

Não tenha cuidado com o que descarrega;

Links e banners: sempre a clicar.



# Debate

**Existem sistemas 100% seguros?**

**O que fazem para proteger os vossos dados pessoais?**

**Quais as rotinas diárias, verificações e comportamentos gerais necessários para se manter seguro online?**

**Porque adotamos um comportamento online diferente do comportamento físico?**

**Deve ter uma atitude crítica e suspeitar de tudo?**