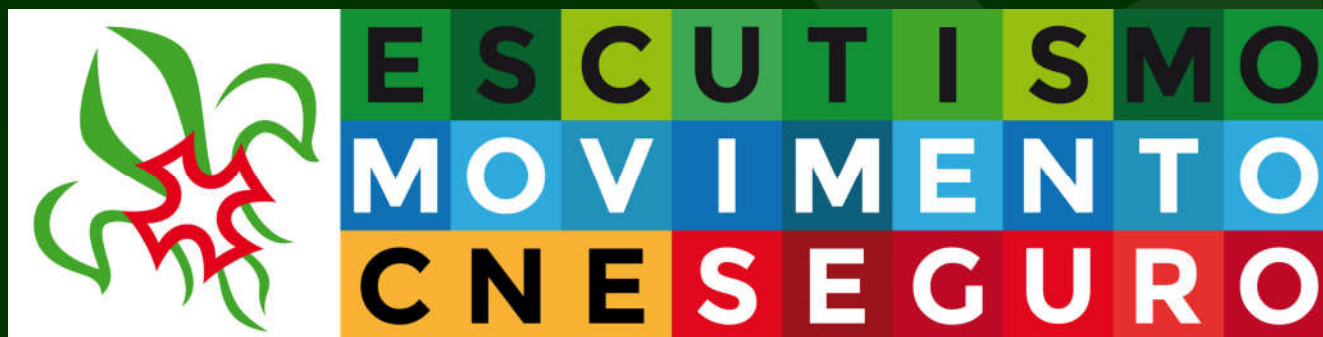


1st Aveiro ScoutSummit



17 de novembro de 2018

Marcos Gonçalves
São Jacinto



INTERNET SEGURA

TÓPICOS

- Conceitos e definições
- Enquadramento legal
- Dados nacionais / internacionais
- Fatores de risco / fatores de proteção associados
- Estratégias de prevenção

Desafio – Teatro

Post-it's comportamento

- O Aspirante: recebeu o seu 1º telefone
- A ExpoPio: a “master” das redes sociais que está fora de prazo na Expedição (Insta, FB,)
- O Ned: sabe tudo sobre o telefone
- O Gamer: domina a ciência dos jogos
- A organizada: usa o telephone para comunicar recados, to-do lists, etc, ..

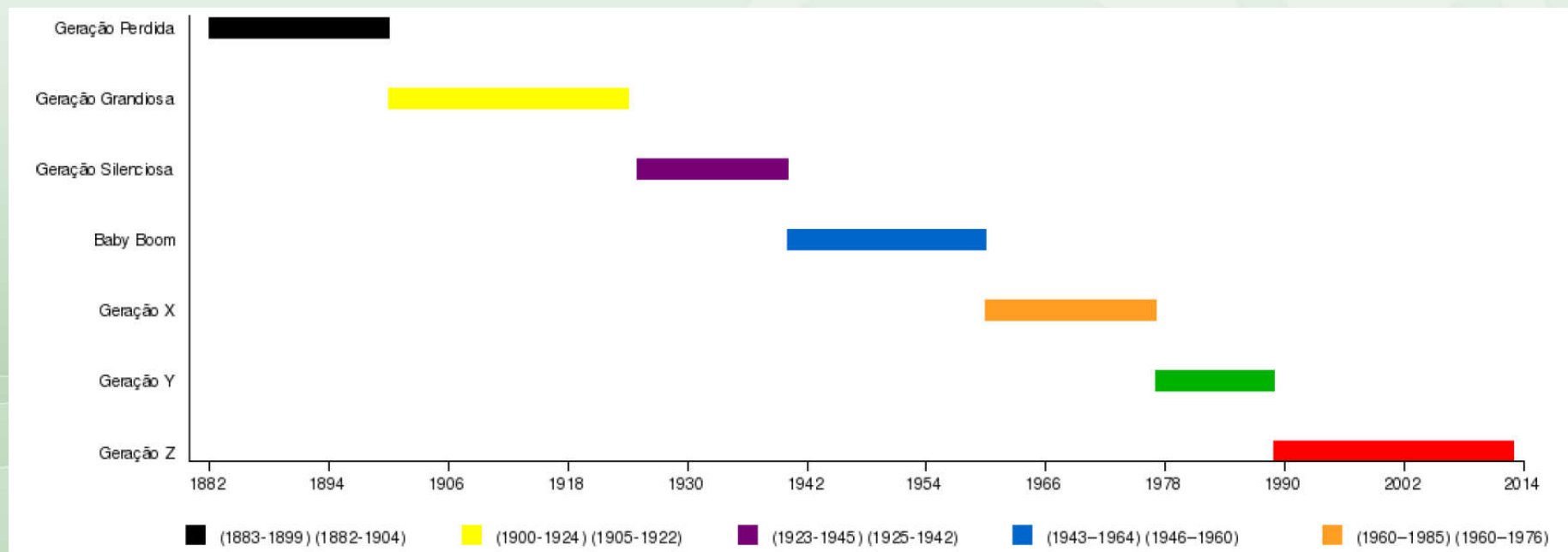
CONCEITOS

Diagnóstico actual

Jovens => Gen Z / Centennials => nativas digitais

Animadores => Millenials => domínio vertente virtual

Geração X => assistiram à criação do mundo digital



ERA DIGITAL

Um mundo de oportunidades

a redução de custos, diminuição de tamanho de equipamentos e agregação de várias capacidades no mesmo aparelho



Telemóvel



GPS



Game Boy



Micro Computador



Máquina fotográfica



CD Walkman



MUNDO DIGITAL

Internet of things



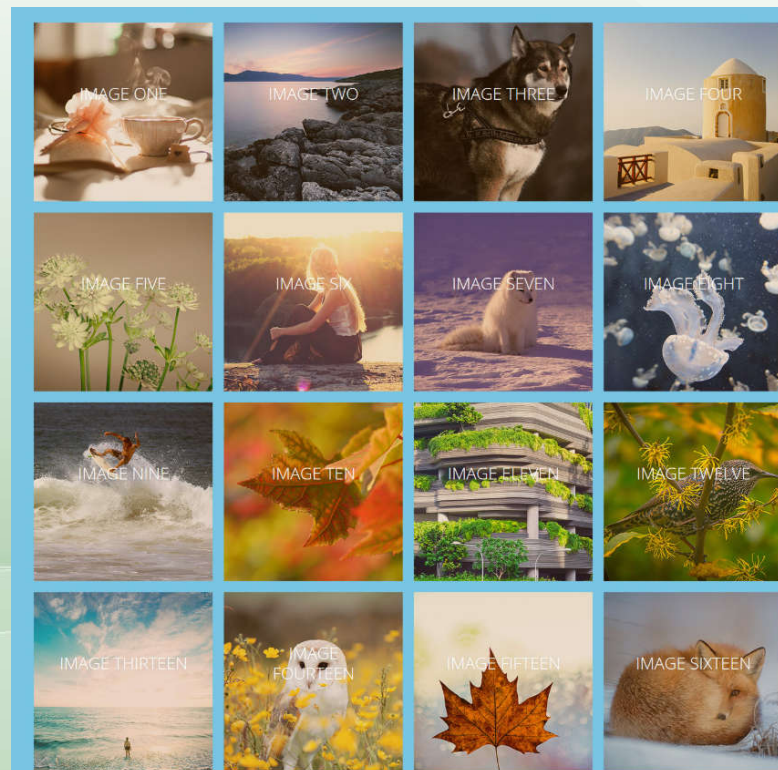
Groupie Time



SAMIR & VIKTOR - GROUPE

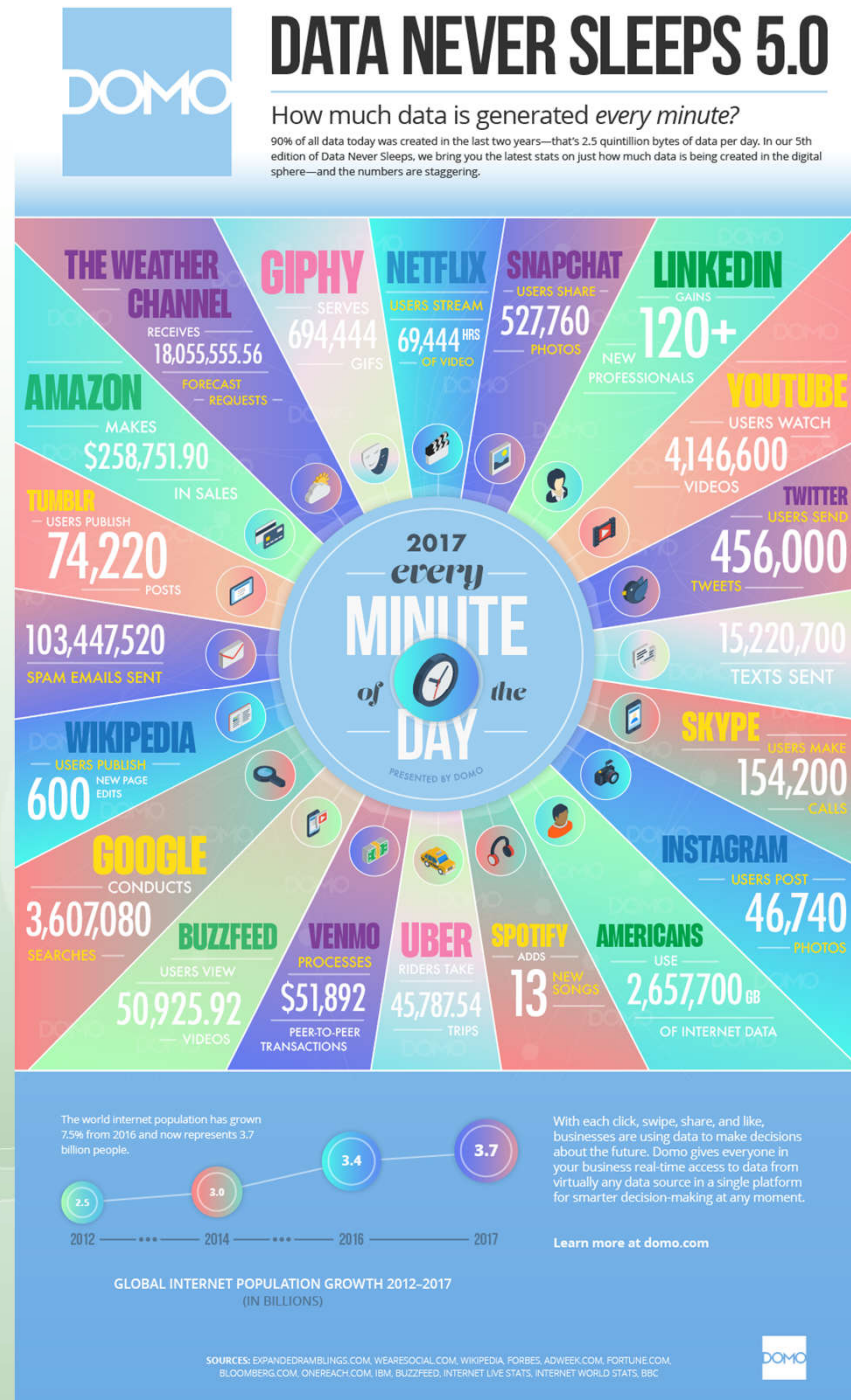
FOTOS

Atualmente, tiram-se mais fotos num dia que no total dos primeiros 100 anos da história da fotografia.



Crescimento
 dados no mundo
 2.5 Exabytes
 por dia

1 EB = 1.073.741.824 GB



Oportunidades educativas

- Redes sociais
- Recursos educacionais (sites, livros, vídeos, músicas, etc, ...)
- Entretenimento (TV, jogos, etc, ... ?)
- Participação cívica e política
- Envolvimento em comunidades
- Domínio e literacia tecnológica

E NÓS ?

Como os Animadores vão conseguir lidar com isto ?

- Informação
- Formação

Como um jovem olha para um adulto que é analfabeto ?

PERIGOS GENÉRICOS

Riscos comparáveis à vida real

- Cyberbullying
- Notícias falsas
- Discursos de ódio
- Sexting
- Internet dos Brinquedos
- Aliciamento
- SPAM / Virus
- Pirataria / Roubos

PERIGOS GENÉRICOS

- Flaming – ataques pessoais e hostis a indivíduos ou grupos, através de mensagens, como por exemplo discussões em fóruns públicos
- Harassment (assédio) - Envio repetido de mensagens insultuosas e desagradáveis
- Denigration (difamação) – divulgação de rumores com o intuito de lesar a reputação
- Impersonation (representação) – Fazer passar-se por outra pessoa e enviar ou publicar material de forma a prejudicá-la . Também nesta categoria temos o **catfishing** – criação de falso perfil para atrair alguém para relacionamento que não corresponde à verdade
- Outing – Divulgação online de segredos, de informação constrangedora ou de imagens
- Trickery – Falar com alguém online no sentido de obter informação pessoal e depois divulgá-la
- Exclusion (exclusão) – Excluir alguém de um grupo online de forma intencional e cruel

PERIGOS GENÉRICOS

- Cyberstalking – Assédio repetido e intenso de forma a denegrir e a provocar medo na vítima
- Happy Slapping – grupos de jovens agredirem alguém com uma bofetada, cuja vítima pode ou não ser conhecida do ofensor, e o incidente ser gravado por jovens desse mesmo grupo através de telemóveis.
- Sexting – envio ou publicação de fotografias ou vídeos de alguém em poses de nudez ou semi-nudez
- Photoshopping – manipulação de imagens, colocando a vítima em ambiente comprometedor
- Confession Pages – páginas com partilha de segredos ou rumores
- Tagging and Untagging - associação de tags a videos, posts ou imagens, de vítimas, em situações fora de contexto para prejudicar a vítima
- Physical threats (Ameaças físicas)

PERIGOS NO ESCUTISMO

- Cyberbullying
- Isolamento na tecnologia
- Dependência (jogos, redes sociais, etc, ...)
- Proibição / restrição de equipamentos eletrónicos em atividades

RESPONSABILIDADES

Código Penal

Artigo 192.º Devassa da vida privada

1 — Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:

- a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada; ⁽¹⁰⁸⁾
 - b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;
 - c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
 - d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;
- é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 — O facto previsto na alínea d) do número anterior não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante.

RESPONSABILIDADES

Código Penal

Artigo 199.º

Gravações e fotografias ilícitas

1 — Quem sem consentimento:

- a) Gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; ou
- b) Utilizar ou permitir que se utilizem as gravações referidas na alínea anterior, mesmo que lícitamente produzidas;

é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 — Na mesma pena incorre quem, contra vontade:

- a) Fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado; ou
- b) Utilizar ou permitir que se utilizem fotografias ou filmes referidos na alínea anterior, mesmo que lícitamente obtidos.

3 — É correspondentemente aplicável o disposto nos artigos 197.º e 198.º.



Enquadramento Legal

Lei Tutelar Educativa (Lei n.º 166/99, alterada pela Lei n.º 4/2015)

Estatuto do Aluno e da Ética Escolar (Lei n.º 51/2012)

Decreto-Lei n.º 401/82 => REGIME PENAL APLICÁVEL A JOVENS DELINQUENTES (16 a 21 anos)

Regulamento Geral de Proteção de Dados

Regulamento (UE) N.º 2016/679, de 27 de abril de 2016

Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

Enquadramento Ético

Qual a política do CNE para uma “utilização segura das tecnologias” ?

O CNE

- educa para o **uso responsável** das tecnologias de informação de modo adequado à idade e maturidade dos escuteiros;
- **privilegia os meios de comunicação coletivos**, designadamente na relação adulto-criança;
- **usa com segurança e responsabilidade as imagens** captadas em atividade escutista, dentro do enquadramento legal e regulamentar vigente;
- **regulamenta, ao nível local, a utilização de telemóveis em atividade escutista**, comunicando-o claramente às crianças e jovens e respetivos encarregados de educação, desde a sua adesão ao movimento.

https://www.youtube.com/watch?time_continue=4&v=oH5YxweS9U8

Boas práticas proteção

NÃO FAZER

- Fornecer dados pessoais próprios ou de terceiros
- Preencher formulários online com dados pessoais
- Expor demasiada informação em redes sociais ou blogues
- Ler / responder a e-mail's de desconhecidos
- Partilhar senhas de acesso
- Fazer compras online, sem supervisão no caso de menores
- Combinar encontros com pessoas que se conheceu online
- Responder a insultos ou comentários desagradáveis
- Usar a internet para magoar, prejudicar ou humilhar alguém



Boas práticas proteção

<http://www.internetsegura.pt/quiz>

Boas práticas proteção

FAZER SEMPRE

- Fornecer o teu email apenas a pessoas que conheces e a entidades que sejam legítimas.
- Atualizar regularmente o antivírus do teu computador.
- Proteger o teu email com um filtro de spam/lixo eletrónico, para evitares receberes emails ou publicidade indesejada ou de destinatários que não te interessam.
- Alterar regularmente as tuas passwords.
- Efetuar sempre logout quando queres sair do teu email ou de uma página da web em que tenhas efetuado login.
- Falar com um adulto em quem confies quando tiver acontecido alguma coisa que te tenha incomodado ou quando tens alguma dúvida.
- Contactar o administrador da página da web em que estás se perceberes que o conteúdo do website é inadequado ou impróprio.
-

Boas práticas proteção

FAZER SEMPRE

- Não responder a qualquer mensagem provocatória ou desagradável e guardar essa informação para a enviar ao administrador do website ou fórum, quando são mensagens de ataque pessoal
- Quando se fazem compras utilizar MBWay, cartões virtuais de uma única utilização e se possíveis plataformas de pagamento seguras (Paypal, ApplePay, etc, ...), pois existe alguma proteção uma vez que os vendedores são verificados e existem mecanismos de resolução de conflitos.
- Nunca informar o número de cartão de crédito ou senha pessoal de acesso a serviços online, mesmo quando requerido pelas empresas detentoras desse serviço.

Estratégias de prevenção

- Informação

Exemplo de Recursos úteis <http://www.apavparajovens.pt/pt/go/menu-top-como-te-manteres-segura-o-seguranca-na-internet>
<http://www.internetsegura.pt/apresentacoes>

- Formação dos Adultos e Jovens para uma cultura ética
https://www.youtube.com/watch?time_continue=21&v=jDMiCOR4Vbc
- Envolver os pais no acompanhamento dos filhos, propondo uma análise crítica e uma atitude construtiva com ética e moral
- Pensar com ponderação na publicação de conteúdos (passados e futuros)
- Eliminar conteúdos não autorizados, publicados ou não, mitigando eventual *hacking* dos aparelhos

Estratégias de atuação

- Quando identificamos situações ilegais ou vitimas
- Comunicar o quanto antes às entidades policiais.
- registar:
 - O que aconteceu
 - Quando aconteceu
 - Onde aconteceu
 - Como aconteceu
- reportar:
 - Aos pais
 - Aos professores / chefes
 - Aos verdadeiros amigos
 - Às autoridades (<http://ww.pj.pt>)
 - À linha Ajuda (<http://www.internetsegura.pt/linha-ajuda>)

número gratuito 800 21 90 90.

Sites ilícitos, reportar em <http://linhaalerta.internetsegura.pt/>