.NET.VIVA. & SEGURA.

Aprende a dominar os domínios da net

Conceitos, truques e dicas para te moveres online de forma segura

UM PROJETO CONJUNTO

Google DECO PROTESTE DEFESA DO CONSUMIDOR

Um projeto conjunto

Google

DECO PROTESTE
DEFESA DO CONSUMIDOR

Com a parceria

REPÚBLICA PORTUGUESA | EDUCAÇÃO

direção-geral da educação

REPÚBLICA PORTUGUESA
CULTURA

IGAC INSPEÇÃO-GERAL DAS ATIVIDADES CULTURAIS

LER+ PLANO NACIONAL DE LEITURA 2027

REDE DE BIBLIOTECAS ESCOLARES

ERTE Equipa de Recursos e Tecnologias Educativas

.pt

Centro Internet Segura

anpri
Associação Nacional de Professores de Informática

O mundo digital é uma realidade (diária) para uma larga maioria dos portugueses. Ele apresenta-se ubíquo e pleno, mas encerra em si mesmo consequências – positivas e negativas – que transcendem o plano virtual e se tornam bem reais. E se é uma inegável verdade que o mundo digital trouxe muitas vantagens (e conforto) para os utilizadores, trouxe também um conjunto de perigos que eram desconhecidos há vinte anos.

Hoje somos confrontados com o comércio ilegal de (dezenas de milhares de) dados roubados, com a invasão dos sistemas, com a adulteração de terminais multibanco, com a corrupção de serviços de pagamentos móveis através de malware, com o ransomware e, claro, com o infame phishing.

E as motivações destes criminosos são tão variadas como a obtenção do vil metal (dinheiro), o desejo de obter informação ou simplesmente a (sádica) intenção de causar disrupção no normal funcionamento de serviços e empresas. Mas também elas são reais.

Ora, se é verdade que muito está a ser feito a montante no sentido do reforço das defesas cibernéticas pelos grandes players digitais (seja um gigante tecnológico como a Google ou pequenas e médias empresas que oferecem bens e serviços junto dos consumidores), a jusante os consumidores digitais não se podem bastar com o conhecimento (teórico) das ferramentas para se protegerem, devem utilizá-las. Não basta saber o que devemos fazer. Temos de o fazer. E todos os dias.

É neste enquadramento que surge o projeto Net Viva e Segura, uma parceria entre a Google e a Deco Proteste – e outrossim este eBook – que visa apresentar e compilar um conjunto de conselhos muito fáceis, oferecidos numa lógica step-by-step, que visa tornar fácil o que se acha difícil, desmistificando alguns conceitos e derrubando algumas resistências (mais ou menos) naturais.

Com este projeto e com a sua integração junto das escolas, temos a clara ambição de ajudar de forma decisiva a promover a literacia digital dos mais jovens, bem como alertá-los para os seus direitos digitais, ao mesmo tempo que procuramos incentivá-los a usarem a Internet de forma segura e a participarem ativamente no desenvolvimento dum mundo digital mais ético.

Rita Rodrigues
Diretora de Relações Institucionais
DECO PROTESTE

Janeiro 2022

Índice

06 Partilha com cuidado

13 Cuidado com as fraudes

16 Privacidade na rede

23 Ser cortês é fixe

31 Pede ajuda

33 Ligações seguras

Introdução

Vivemos num mundo online. O número de portugueses que usa a Internet continua a crescer de ano para ano. Hoje, três em cada quatro portugueses utilizam a Internet todos os dias. E cada vez mais o acesso à Internet é feito em mobilidade através de smartphones, segundo 80% dos utilizadores (o que representa o dobro quando comparado com a realidade de há cinco anos).

Partilha de forma segura: não brinques com a tua privacidade.

Vários estudos da DECO PROTESTE destacam que a preocupação com a privacidade e a segurança online tem aumentado. Navegar na internet e usufruir das redes sociais de forma segura é mais fácil do que parece.

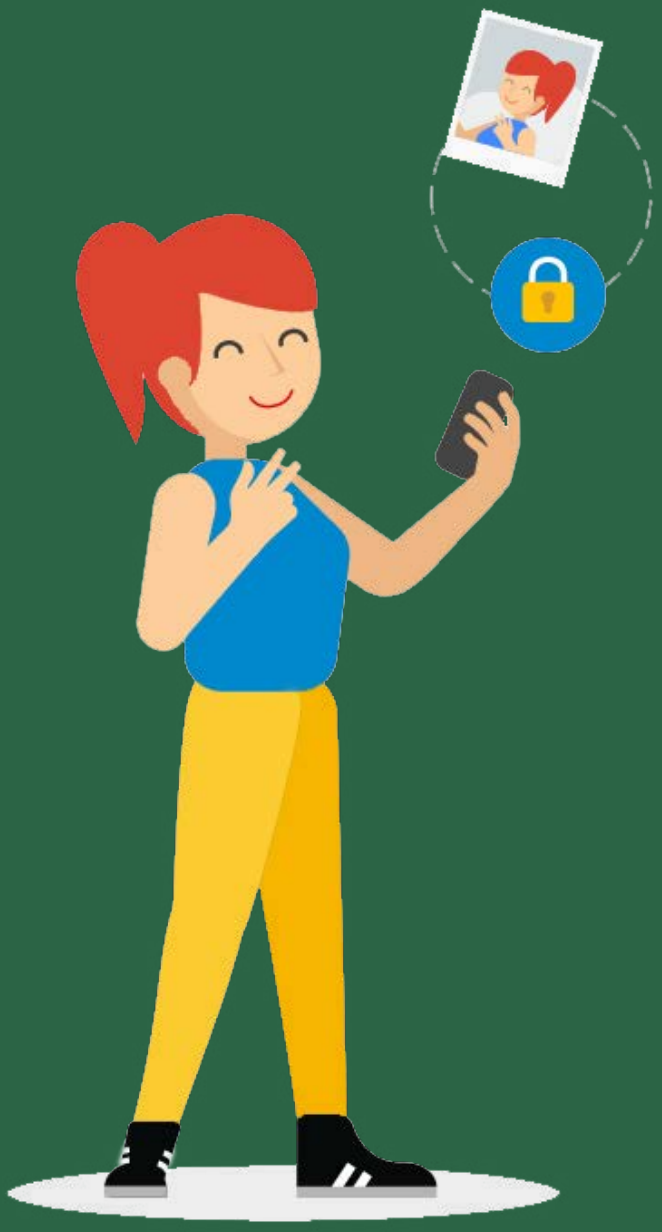
Está nas tuas mãos: toma medidas e protege-te.

Existem ferramentas para proteger a tua segurança e privacidade na internet. Damos-te alguns conselhos muito práticos para gerir a tua informação e partilhas nas redes sociais.

Contamos-te todos os segredos para utilizares as redes sociais de forma mais segura.

PARTE UM: PARTILHA

Partilha com cuidado



01

Partilhar sem correr riscos

1. Porque é que a privacidade interessa

A tua pegada (ou presença) digital representa quem tu és online.
Isto abrange fotos, áudio, vídeos, mensagens, gostos e comentários em publicações nos perfis dos teus amigos.

Vantagens e Riscos

A internet faz com que seja mais fácil comunicar com a família, amigos e pessoas que gostam das mesmas coisas que tu. Enviamos mensagens, partilhamos fotos e falamos em redes sociais – muitas vezes sem nos apercebermos que há mais pessoas que também podem ver o que partilhamos.

Partilha com cuidado

Uma fotografia ou uma publicação que achas engraçada e inofensiva hoje, pode ser vista e interpretada de forma diferente por pessoas que nunca pensaste que poderiam ver esse conteúdo – hoje ou no futuro. Assim que uma coisa cai na internet, é muito difícil voltar atrás.

O que é a reputação digital

A tua reputação digital é o conjunto de ideias, opiniões, impressões ou crenças que os outros têm sobre ti. Pode ser descrito como algo sobre o qual não tens a certeza absoluta mas que geralmente queres que seja visto como positiva ou boa pelos outros.

Quando não devo partilhar

Como tudo na internet, a tua pegada digital pode ser vista por pessoas que tu nunca conheceste. Assim que dizes ou fazes alguma coisa online, ela pode lá ficar para sempre. Pensa muito bem sobre o que publicas e partilhas online. E pensa que, algumas vezes, o melhor é mesmo não publicar (como, por exemplo, reagir a quente a publicações de outros).
Já todos ouvimos que devemos “pensar antes de publicar" e se já todos ouvimos, é porque é mesmo um bom conselho.
A melhor maneira de respeitares a tua privacidade e a dos outros é pensares sobre o que é OK de publicar, quem pode ver a tua publicação, que efeitos pode ter nos outros e quando não deves publicar de todo.

2. Atenção e cuidado ao partilhar alguns tipos de informação

Muita atenção e cuidado ao partilhar alguns tipos de informação

Deves ter cuidado ao partilhar informações pessoais ou sensíveis na internet, especialmente quando não sabes com quem o estás a fazer. Há informações e dados que é melhor guardares para ti.

Detalhes pessoais que te permitem identificar

Algumas redes sociais precisam do teu nome e número de telemóvel para o efetuares o registo. Mas para além das informações básicas, evita partilhar outras, tais como o nome do meio, número do cartão do cidadão, a tua morada, os nomes dos teus animais de estimação, a data do teu aniversário, as escolas que frequentaste, etc.

Onde e quando vais de férias

Usamos as redes sociais para partilhar fotos, vídeos, curiosidades e outras tantas coisas, mas não devemos partilhar informações detalhadas sobre onde e quando vamos estar de férias.

Ao fazê-lo, podes estar a abrir uma janela de oportunidade para que ladrões te assaltem a casa. Podes publicar fotos das férias à vontade, mas fá-lo sem grandes informações ou de preferência quando já estiveres de regresso a casa.

Compras que fizeste

Quanto mais extravagantes são as compras que fazes, mais cuidados deves ter em partilhá-las nas redes sociais. A exposição em excesso pode atrair atenções indesejadas. O melhor conselho é que tornes o teu perfil privado. Assim garantes que só os teus amigos poderão ver as tuas publicações.

3. Quem é quem online

Quem é quem atrás do anonimato digital

O anonimato funciona como um combustível bastante volátil nas interações digitais. Nunca sabemos com certeza quem está do outro lado. Nem mesmo quando são conhecidos de pessoas com quem te relacionas.

De quem é mesmo este perfil

Sempre que vemos publicações, comentários e fotos de outras pessoas, fazemos considerações pessoais sobre elas e a verdade é que essas nem sempre são corretas, especialmente se não as conhecermos. Tal é assim porque aquilo que vemos online é apenas uma parte do que os outros são e sobre aquilo que os preocupa. Mas também pode ser alguém a fingir ser outra coisa ou um sentimento que foi expresso num determinado momento. A verdade é que não podemos realmente saber quem são e o que sentem as pessoas até as conhecermos pessoalmente – e até nesses casos, leva tempo.

Como é que os outros nos vêem?

Diferentes pessoas podem ver a mesma informação e tirar conclusões diferentes sobre isso. Não assumas que as pessoas nas redes sociais te vão ver da forma como tu pensas que elas te vão ver.

Manter as contas e publicações privadas

Diferentes situações reclamam por respostas diferentes, tanto online como offline. É fundamental respeitar as escolhas privadas das outras pessoas, mesmo que sejam opções que tu não tomarias.

Então o que posso fazer?

Tens de encontrar um equilíbrio e ter consciência dos riscos quando disponibilizas os teus dados. Se o fazes ou não, tem a ver com a tua liberdade e autodeterminação, mas tens de perceber que quando dizes na Internet quem és, o que fazes, onde estás e onde moras, podes colocar em causa a tua impressão digital.

4. O que fazer para a internet esquecer

O que fazer para a internet esquecer

Quando queres garantir que determinadas informações ou uma foto tua é eliminada porque a publicação não teve o teu consentimento, há formas de o fazer. Fica a conhecer algumas:

O que é o direito ao esquecimento?

Direito ao esquecimento é um termo comummente utilizado para nos referirmos à possibilidade de solicitares à Google e a outras empresas detentoras de motores de busca que apaguem URL que contêm os teus dados pessoais quando não há interesse público em que aquela informação permaneça nos resultados de busca. Esta possibilidade tem por base a decisão de 2014 do Tribunal de Justiça da União Europeia (TJUE) de acordo com a qual um motor de busca é responsável pelo processamento dos dados pessoais. Recentemente, o direito ao esquecimento foi reforçado pelo Regulamento Geral de Proteção de Dados (RGPD).

Como posso exercer o direito ao esquecimento?

Para facilitar o envio dos pedidos, a Google disponibilizou um formulário online acessível a todos os europeus. Assim, quem quiser que a Google deixe de mostrar links para conteúdos "inadequados, irrelevantes ou excessivos" sobre si, só tem de requerer e a Google garante que cada pedido será analisado individualmente. Mas se a resposta for negativa, há sempre a hipótese de recorreres aos tribunais ou às autoridades de proteção de dados (em Portugal, a CNPD).

E o pedido do direito ao esquecimento garante que tudo é eliminado?

O problema com a informação e conteúdos que caem na Internet é que esta pode facilmente espalhar-se por vários locais e dispositivos. Basta que alguns utilizadores copiem os dados para o seu computador e voltem a partilhá-los numa outra página. Mas fica a saber que é possível atualizar a lista de desindexação de conteúdo, adicionando novos sítios onde o conteúdo possa ter sido novamente partilhado e assim eliminá-lo.

5. Protege o teu dispositivo

Protege o teu dispositivo

Certamente que não queres que ninguém leia as tuas mensagens ou aceda à tua agenda. Como evitá-lo? Protegendo o teu telemóvel. Dizemos-te o que fazer!

Como utilizar o método de encriptação nos dipositivos?

Não entres em pânico, é muito simples! Vê como, dependendo do sistema que utilizas. Mas não te esqueças de carregar a bateria!

Android:

1. Em «Definições», seleciona a opção «Segurança».
2. Dentro de «Segurança», seleciona «Encriptação». Se encontrares o conceito «Telefone encriptado» não te assustes, significa que o teu dispositivo já está seguro; caso contrário, terás de carregar em «Encriptar telefone».
3. A última coisa a fazer é escolher uma boa palavra-passe. E não, o nome do teu animal de estimação não serve, é demasiado fácil.

iOS:

1. Em «Definições» seleciona a opção «Touch ID e Código».
2. Neste passo, podes alterar a palavra-passe do teu dispositivo ou criar uma nova impressão digital. Para isso, carrega em «Adicionar impressão digital» ou «Alterar código».

Windows:

1. Em «Painel de Controlo» entra em «Sistema e Segurança» e acede a «Encriptação de Unidade BitLocker».
2. Escolhe o dispositivo que pretendes encriptar e seleciona «Ativar BitLocker».

Mac:

1. No menu Apple, escolhe «Preferências do sistema» e depois «Segurança e Privacidade».
2. Clica no separador «FileVault» e depois no ícone do cadeado.
3. Por último, introduz o teu nome e palavra-passe e clica em «Ativar FileVault».

Linux:

Basta localizar as várias ferramentas de encriptação oferecidas pelo sistema.

6. Protege os teus dados privados com a encriptação

Protege os teus dados privados com a encriptação

Garantirás a privacidade dos teus dados para que ninguém tos possa roubar. A encriptação é um sistema através do qual proteges os teus dados e evitas que te roubem informações privadas.

O que posso encriptar?

Podes encriptar o teu email, o acesso a páginas web, ligações a outros dispositivos remotos, etc., e qualquer serviço de Internet que queiras proteger. Normalmente, é aconselhável utilizar a encriptação em todas as comunicações em que se trocam dados pessoais, palavras-passe de utilizador, informação financeira, etc.

Como funciona a encriptação de dados?

A encriptação é feita através do SSL, que é o protocolo que normalmente se utiliza para encriptar.

Como posso saber se os meus dados estão encriptados?

Há fornecedores, que encriptam os seus serviços para proteger a sua informação. Podes verificar se estás a usar um serviço de encriptação da seguinte forma:

1. Verifica se no endereço da página web em que te encontras aparece **https://** e não http://.
2. Se aparecer um cadeado na barra de estado do teu navegador, isso significa que é uma navegação segura.

PARTE DOIS: FRAUDES

Cuidados com as fraudes

02

As fraudes e os perfis falsos são bem reais

1. Não mordas o anzol do phishing

A internet e as redes sociais representam oportunidades incríveis e revolucionaram a forma como comunicamos, mas também escondem práticas ilegais, para as quais é importante que estejas alerta.

O que é o phishing?

O phishing acontece quando alguém tenta roubar informações como as tuas palavras-passe ou códigos multibanco fingindo ser alguém em quem confias através de um email, mensagem ou outra forma de comunicação online. Os emails de phishing (e os sites inseguros para os quais te podem remeter ou os anexos que podem querer que abras) podem, igualmente, trazer vírus para o teu computador ou telemóvel.

O que fazer para evitar o phishing?

Antes de clicares num endereço ou colocares a tua palavra-passe num site em que nunca estiveste antes, é boa ideia perguntares a ti mesmo algumas questões sobre aquele email ou site:

- Parece profissional como outras páginas da Internet que conheces e confias?
- O endereço URL coincide com os produtos ou o nome da empresa e a informação que estás à procura?
- O URL começa com https:// precedido de um pequeno cadeado?
- Há pop-ups do estilo de spam?
- O email ou a página de Internet estão a oferecer uma coisa que soa demasiado boa para ser verdade (como a hipótese de ganhar dinheiro sem esforço)?
- O texto tem gralhas ou erros ortográficos grosseiros ou parece ser uma tradução mal conseguida?

O que fazer quando foste vítima de uma fraude?

Antes de mais, não entres em pânico.

- Conta imediatamente aos teus pais, professores ou a algum adulto em quem confies. Quanto mais esperares, pior será.
- Muda as tuas palavras-passe em todas as tuas contas online.
- Se foste enganado numa fraude, avisa rapidamente os teus amigos e pessoas na tua lista de contactos porque eles podem ser os próximos alvos.
- Sempre que possível, usa as definições para reportar a mensagem ou email como spam.

Quantos tipos de phishing existem?

Para além da forma mais tradicional de phishing há ainda outras variantes, sendo as mais comuns as que se seguem:

Spearphishing é uma fraude em que um atacante te tem como um alvo mais preciso e onde é utilizada a tua própria informação pessoal.

Catphishing é uma fraude em que é criada uma identidade ou uma conta falsa numa rede social para enganar as pessoas e levá-las a partilhar a sua informação pessoal ou a fazê-las crer que estão a falar com uma pessoa real atrás duma conta, perfil ou página verdadeira.

Clickbait é a técnica de utilizar fraudulentamente conteúdos, publicações ou anúncios manipulativos online com o objetivo de captar a atenção das pessoas e levá-las a clicar num endereço ou num link, a maior parte das vezes para aumentar o número de visualizações ou o tráfego da página no sentido de fazer dinheiro.

PARTE TRÊS: PRIVACIDADE

Privacidade nas redes sociais

03

Não partilhes a tua vida toda nas redes sociais

1. Escolhe o que pretendes que saibam de ti

Por vezes, não temos consciência de que podemos partilhar informações na Internet às quais muitas pessoas podem ter acesso, principalmente quando não usamos configurações de privacidade Por isso, pensa bem antes de publicar uma foto ou informação comprometedora nas tuas redes sociais.

Faz uma gestão cuidadosa daquilo que realmente queres que se saiba sobre ti publicamente. É possível que não queiras que toda a gente veja as tuas fotos da festa de sábado. Para isso, podes escolher o que partilhar e com quem. Não brinques com a tua privacidade!

Como gerir seus dados em alguns serviços em linha?

A minha conta Google:
alterar a privacidade para o que mais te convém é muito fácil. Além disso, podes aceder às opções de privacidade e segurança dos teus dados em todas as contas Google muito rapidamente.

Facebook:
também permite gerir o funcionamento da tua privacidade. Vai ao ícone do cadeado que aparece no canto superior direito e escolhe.

LinkedIn:
se não queres que a tua conta apareça nos motores de pesquisa, podes geri-lo no teu perfil em "privacidade e partilha" e assim evitar que alguém te encontre nesta rede profissional.

Twitter:
na secção «Privacidade e segurança» tens várias opções para controlar quem te pode marcar, mencionar, ver a localização... e outros dados que talvez não queiras mostrar em público.

Instagram:
dada a natureza fotográfica desta rede, a gestão da privacidade pode ser muito útil. Se pretendes configurar os parâmetros de privacidade, deves premir o botão «Definições» e escolher a opção «Conta Privada». Desta forma, só as pessoas que aceitares é que poderão ver as tuas fotos.

WhatsApp:
para escolher se queres partilhar a hora da tua última ligação, a tua foto de perfil ou se leste as mensagens, vai a «Definições» (Android) ou «Configurações» (iOS), depois «Conta» e por último «Privacidade».

Posso pedir que os motores de busca eliminem o meu nome das pesquisas?

Uma sentença do Tribunal de Justiça da União Europeia determinou, em 2014, que é possível, mas apenas se os resultados mostrados forem inadequados, irrelevantes ou excessivos. Se precisares de mais informações, consulta o site da CNPD (Comissão Nacional da Proteção de Dados).

2. Não deixes os teus dados à solta por aí

Certamente que não deixas os teus álbuns de fotos por aí, à vista de qualquer pessoa. Pois deverias fazer o mesmo na internet, pois a sua distribuição massiva pode ser feita com uma rapidez impressionante. Aprende como controlar quem pode ver as tuas fotos e dados.

Não aceites pessoas que não conheces nas tuas redes sociais

As redes sociais facilitam as relações, a comunicação e o poder localizar antigas amizades. Mas cuidado: se não conheces a pessoa que te deseja adicionar como amigo, é melhor não a adicionares, pois pode ser qualquer um. Ou deixas entrar desconhecidos em tua casa? Pois se não deixas a chave na porta, também não o faças com os teus perfis pessoais.

Evita publicações indesejadas

Já te deve ter acontecido mais do que uma vez um amigo ter-te identificado numa foto em que não ficaste bem. Para evitar essas situações, escolhe a identificação tanto das fotos como das publicações.

Ou seja, é possível autorizar as publicações em que queres aparecer.

Como controlar a identificação

É muito simples, vê como fazer para cada uma das redes sociais.

Facebook:
vai a «Definições» e depois a «Cronologia e identificação» para selecionares o tipo de identificações que pretendes. Para mais informações, segue esta ligação.

Twitter:
vai a «Marcação de Foto» dentro de «Privacidade e segurança».

Instagram:
qualquer pessoa pode identificar-te em fotos, a menos que a tenhas bloqueado. No entanto, revê o «Centro de privacidade e segurança» dentro do menu «Ajuda» para veres as diferentes opções de que dispões para preservar a tua privacidade.

3. Pensa bem antes de dizeres onde estás

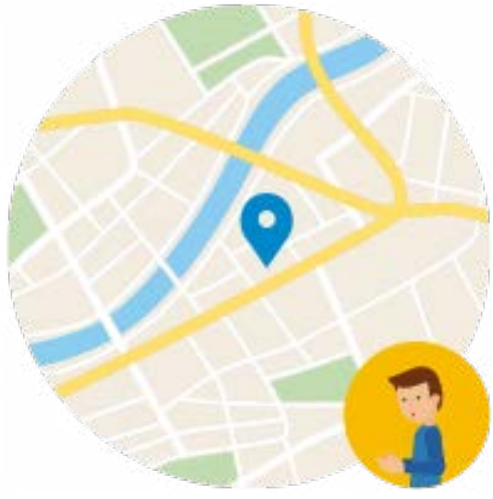
Estamos de acordo quanto ao facto de os serviços de geolocalização ou check-in serem muito úteis em alguns casos. Mas contar constantemente onde estamos pode ser utilizado contra nós. Pode ser muito útil quando temos de partilhar com um amigo a nossa localização, ou quando queremos informar sobre o evento em que estamos nesse momento. O problema surge quando este tipo de informação é aproveitado com más intenções, por exemplo, por ladrões que aproveitam a nossa ausência para entrar em nossa casa.

Sabes onde estão as configurações dos serviços de geolocalização?
Se não sabes, nós ajudamos. Mas lembra-te que os passos a seguir dependem do tipo de plataforma que utilizas:

Android
vai à secção «Localização» a partir de «Definições». Podes desligar totalmente os serviços de localização quando quiseres. É fácil!

iOS
permite-te personalizar, dependendo de cada aplicação, ou seja, podes desativar a geolocalização por aplicações. Para isso, vai a «Localização» e seleciona quais as aplicações que queres que mostrem a tua localização. Esta secção encontra-se em «Definições» e «Privacidade».

Windows Phone
podes configurar a tua localização a partir da própria aplicação quando estiveres a utilizar este serviço ou desativá-la por completo a partir do menu «Serviços de Localização» dentro de «Definições».



Firefox
a própria plataforma pergunta-te se pretendes ativar ou desativar a geolocalização. Se tiveres tido algum problema e te tiveres esquecido deste detalhe, não te preocupes, podes desativar a tua localização da seguinte forma: escreve «about:config» na barra de endereços, utilizando o motor de busca que aparece na parte superior, procura a entrada geo.enabled = false e desativa a geolocalização.

Blackberry:
basta aceder a «Serviços de localização» e escolher o estado «Ativado» ou «Desativado». Podes encontrar esta secção em «Definições», dentro do menu «Serviços de localização».

Complicado? Esperamos que não e que a partir de agora tenhas mais cuidado ao divulgar onde te encontras.

4. Atualiza o teu navegador

Atualizar o navegador não custa nada e pode ajudar a evitar possíveis perigos na rede. Por isso, já sabes!

Como atualizar o navegador

Atualizar o navegador é uma medida de segurança para evitar que os teus dados privados fiquem gravados na rede. Não te preocupes, a maioria atualiza-se de forma automática. Caso tenhas de o fazer manualmente, é relativamente rápido e pode poupar-te várias dores de cabeça.

PARTE QUATRO: CORTESIA

Ser cortês é fixe

04

A cortesia nunca sai de moda

1. A cortesia não é uma fantasia

O mundo digital cria novos desafios e oportunidades para interagirmos socialmente. Mas é muito mais difícil ler o tom nas comunicações digitais do que numa conversa cara a cara. E claro que, por estarmos constantemente ligados, isso nos traz conforto e ansiedade ao mesmo tempo.

A cortesia não é uma fantasia

A cortesia é um pilar fundamental nas interações positivas no mundo digital e, em particular, nas redes sociais. É também uma das melhores armas contra a maldade e negativismo que grassam na Internet.

Porque é importante ser cortês online

Nunca deves esquecer que atrás de um "username" está uma pessoa real, com sentimentos reais. A regra de ouro é que devemos tratar os outros como gostaríamos que nos tratassem.

Mas a cortesia online é assim tão importante?

Já sabes que a Internet e as redes sociais podem amplificar a bondade e a maldade. Por isso é importante aprenderes a transmitir empatia – mas também como deves responder a comentários maldosos e ao assédio – porque isso é essencial para construíres relações saudáveis e reduzires possíveis sentimentos de isolamento que podem conduzir a situações de bullying, depressão, dificuldades nos estudos e outros problemas.

Como posso ser cortês nas interações digitais?

Acreditamos que mais importante do que te dizer que não deves ser negativo nas redes sociais, a prevenção passa por encorajar os jovens a interagirem de forma positiva online, bem como mostrar-lhes as melhores formas para lidarem com a maldade e o assédio quando elas surgem. A melhor forma de transmitir cortesia passa por expressares os teus sentimentos e opiniões de forma positiva e responderes a comentários e publicações negativas de forma construtiva e civilizada.

2. O bullying é uma triste realidade

O assédio, seja como bullying, cyberbullying, intimidação ou gozo cruel e ofensivo, é uma realidade que te pode afetar a ti e aos teus colegas.

O que é o bullying

O bullying pode ser descrito como um comportamento maldoso propositado e reiterado. A vítima ou alvo de bullying tem muitas vezes dificuldades em defender-se do agressor.

O que é o cyberbullying

O cyberbullying é o bullying que acontece online, nas redes sociais ou através de dispositivos eletrónicos.

Que tipos de pessoas há numa situação de bullying

Há geralmente quatro tipos de pessoas envolvidas numa situação de bullying ou de cyberbullying:

1. O agressor, que é quem pratica o bullying;
2. A vítima ou alvo, que é quem sofre as consequências do bullying;
3. O observador passivo, que é quem vê o bullying mas opta por não intervir;
4. O observador ativo, que é quem vê o bullying e decide apoiar, publicamente ou em privado, a vítima, podendo até tentar pôr um fim à agressão e/ou reportar o que testemunhou.

O que fazer se fores alvo de bullying

Se fores vítima de bullying ou de outros comportamentos negativos online, tens algumas opções:

- Podes optar por não responder
- Podes bloquear a pessoa em questão
- Podes reportar as pessoas que te estão a importunar, seja aos teus pais, irmãos, professores ou qualquer outra pessoa em quem confies, e utilizar as ferramentas de reporte na rede social ou na aplicação em questão e denunciar a publicação, o comentário ou a foto que te está a causar mal-estar.

O que deves fazer se assistires a um caso de bullying

Se testemunhares um caso de assédio ou de bullying tens a capacidade de intervir e reportar esse comportamento negativo.

Muitas vezes, os observadores passivos não tentam pôr um travão à situação de bullying, nem ajudam a vítima, mas quando o fazem transformam-se em observadores ativos. Para seres um observador ativo basta que te oponhas a comportamentos negativos e que apoies a bondade e a cortesia. Um bocadinho de bondade pode ir muito longe online. E pode impedir que a maldade se propague e se transforme em crueldade.

Como posso passar de um observador passivo a ativo

Para te transformares num observador ativo, basta que:

- Encontres uma forma de ser cortês para a vítima de bullying ou a apoies de alguma forma;
- Que chames a atenção para o comportamento negativo num comentário ou numa resposta – mas lembra-te que deves focar-te no comentário ou na publicação e não na pessoa – se te sentires confortável com isso e se for seguro;
- Decidas não apoiar o agressor, bastando que não divulgues o bullying nem partilhes as publicações ou os comentários negativos nas redes sociais;
- Reúnas um grupo de amigos para criar uma pilha de cortesia, ou seja, que publiques muitos comentários positivos sobre a pessoa que está a ser alvo de bullying (mas não comentários negativos sobre o agressor, porque estás a dar o exemplo e não a retaliar).
- Denuncies o assédio. Conta a alguém que possa ajudar, como um dos teus pais, um professor ou alguém em quem confies.

Formas de travar o bullying

Dependendo do caso concreto, há várias formas de travares uma situação de bullying e defenderes ativamente as vítimas, seja reportando uma situação de assédio ou ignorando uma situação para, desta forma, impedir que a mesma seja amplificada. Todos temos esta capacidade de, com um bocado de bondade, cuidado e cortesia, fazermos uma enorme diferença nas interações nas redes sociais.

3. Tem cuidado com o tom que usas

O tom que usas não é fácil de decifrar
Sabemos que pode ser difícil perceber como é que outra pessoa se está realmente a sentir quando estás a ler um comentário ou uma mensagem. O tom não é fácil de transmitir num texto, pelo que deves ter particular cuidado com o que escreves.

É muito fácil sermos mal interpretados online

Todos usamos diferentes tipos de comunicação para diferentes formas de interação, mas as mensagens enviadas através de um "chat"/fórum podem ser interpretadas de forma muito distinta do que seriam se fossem ditas pessoalmente ou em conversa telefónica. Por exemplo, já alguma vez escreveste uma piada para um amigo e ele pensou que estavas a falar a sério? Estas situações acontecem a todos e por isso mesmo devemos aprender a minimizá-las.

O que podemos fazer para prevenir más interpretações

Deves refletir muito bem sobre a forma como comunicas e quando comunicas – e, em alguns casos, até evitar comunicar de todo. Há situações em que deves esperar e falar cara a cara com uma pessoa, em vez de lhe escrever imediatamente.

A boa comunicação é um pilar essencial de um mundo digital saudável

A forma como tu e os teus amigos se tratam online vai ter um impacto tremendo na forma como a tua geração vai construir o mundo digital – já para não falar no mundo real.

Como transformar comentários negativos em positivos

Sabemos que és exposto a todo o tipo de conteúdos online, alguns dos quais contêm mensagens negativas e que promovem comportamentos incorretos. Mas deves saber que é possível responder a sentimentos negativos através de uma abordagem construtiva que pode passar por reformulares

ou refreares os comentários menos amigáveis e assim tornares-te mais consciente do tom nas tuas comunicações online.

Evita reações a quente

Quando reages a um comentário negativo de forma positiva, ficas com o poder de direcionar a conversa para um tom mais divertido ou interessante – o que é muitas vezes melhor do que ter de trabalhar para limpar uma confusão criada por comentários menos abonatórios feitos a quente.

4. Lidera pelo exemplo

Os bons exemplos ajudam a guiar os outros

Quando vês alguém a ser maldoso para outra pessoa online – com alguma coisa que as faz sentirem-se desconfortáveis, marginalizadas, gozadas, desrespeitadas ou magoadas – tens sempre escolhas. Podes, desde logo, optar por ser um observador ativo, em vez de passivo, e ajudar a vítima.

O que eu faço é assim tão importante?

Claro que sim! Não te esqueças que para ajudar ativamente alguém que se sinta assediado e triste pode bastar ouvires o que têm a dizer – porque isso vai ajudá-los a perceberem que há alguém que se preocupa.

E se eu quiser fazer mais para ajudar alguém?

Nem todos se sentem confortáveis em defender os outros em público, seja online ou no refeitório da escola. Se não tiveres problemas com isso, força!

Podes:

- Chamar a atenção para o comportamento (e não para a pessoa), dizendo que não é fixe;
- Dizer alguma coisa positiva sobre a vítima de bullying num comentário ou numa publicação;
- Garantir que os teus amigos também elogiam a vítima nas redes sociais;
- Pessoalmente, podes convidar a vítima a estar contigo nos intervalos e/ou a almoçar contigo e com os teus amigos.

Se não te sentires confortável em confrontar a situação de bullying em público, não tem problema. Podes apoiar a vítima em privado.

Podes:

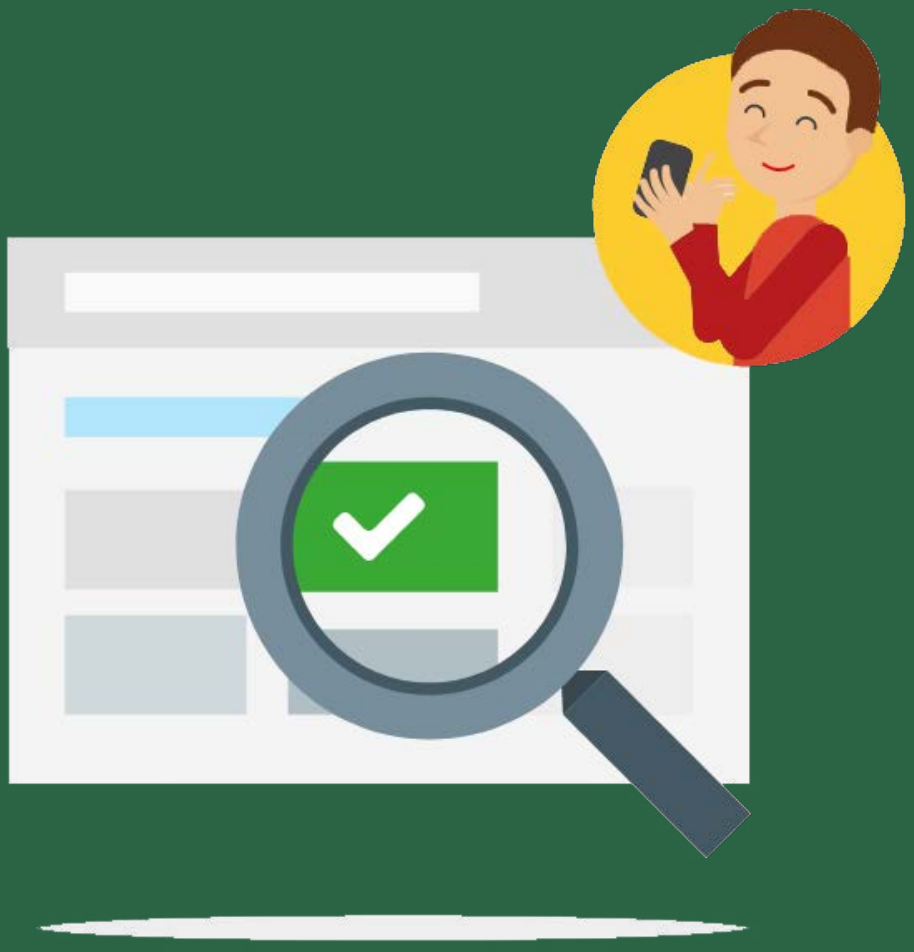
- Perguntar-lhe como se sentem, numa mensagem privada;
- Dizer-lhe um elogio ou um algo simpático num comentário, publicação ou mensagem anónima (se estiveres numa rede social que te permita ficar anónimo);
- Dizer-lhe que estás lá para a apoiar se ela precisar de falar depois da escola;

- Conversar com ela, pessoalmente ou por telefone, e dizer-lhe que achas que o comportamento maldoso foi errado e perguntar-lhe se quer conversar sobre o que aconteceu.

Não interessa como escolhes ser um observador ativo, tens opções de reporte tanto públicas como privadas. Isto significa que tens meios para denunciar uma situação de bullying ou cyberbullying através do interface de uma aplicação ou rede social ou reportar a situação a um adulto em quem confies.

PARTE CINCO: AJUDA

Se precisares de ajuda, pede



05

Pedir ajuda não é cobardia

1. A coragem implica ação

Quanto mais novo é o utilizador das redes sociais, maiores são os perigos que o mundo digital esconde. Mas é importante que saibas que não estás sozinho e que podes pedir ajuda a alguém em quem confies se te sentires ameaçado.

A coragem implica ação

Há várias formas de ser corajoso e atuar. Podes falar com alguém sobre o sucedido e podes utilizar as ferramentas de reporte online das diferentes redes sociais e/ou aplicações.

Quando é que devo pedir ajuda?
A regra de ouro é que: se tens dúvidas, deves pedir ajuda. Nem sempre parece, mas pedir um conselho ou uma opinião sobre alguma coisa que desconheces ou que te deixa desconfortável é um ato de coragem, mas também de inteligência. E não te esqueças que pedir ajuda e "fazer queixinhas" são duas coisas muito distintas.

Como posso pedir ajuda?

Quando algo ameaçador ou inapropriado surge online, tens várias opções. Para além de falares com alguém de confiança, podes reportar a situação junto da rede social ou da aplicação onde deste com a ameaça, mas também podes denunciar a situação junto da polícia. Essa denúncia vai ajudar a eliminar o conteúdo em causa.

Como devo reportar?

Antes de denunciares uma publicação, um comentário ou uma mensagem de cariz suspeito ou ameaçador, deves fazer um "screenshot" dessa atividade antes mesmo de usares as ferramentas de bloqueio ou reporte (porque ao fazê-lo o conteúdo pode ficar inacessível). Assim, garantes que ficas com um registo para mostrar às pessoas em quem confias e que te podem ajudar a resolver a situação.

PARTE SEIS: LIGAÇÃO

Ligação segura

06

Podes ligar-te à internet sem riscos

1. Como proteger o teu router

Sabemos que gostas de navegar na internet, mas será que o fazes com uma ligação segura?

Como proteger o teu router

Se queres manter as tuas conexões seguras e evitar que pessoas indesejadas interfiram com a tua ligação ou que se apoderem dos dados que comunicas através da internet, utiliza um método de encriptação.

Protege o teu router com o método de encriptação

O router de tua casa é o teu meio para te ligares à Internet. Por isso, é imprescindível protegê-lo de ataques que possam pôr em perigo a tua privacidade.

Como posso proteger o meu router?

Os passos a seguir são muito simples e evitarão que tenhas alguns desgostos.
1. Vai à página web do administrador do teu router e introduz o nome de utilizador e a palavra-passe que aparecem no próprio dispositivo.
2. Altera a palavra-passe para uma segura.
3. Nas opções de segurança da rede Wi-Fi, procura os parâmetros que te permitem utilizar autenticação WPA2-PSK e a encriptação AES.
4. Além disso, desativa o modo WPS.

Tenho de alterar as palavras-passe?

É muito importante que este seja um dos teus primeiros passos quando instalas um router. As tuas palavras-passe devem ser pessoais e intransmissíveis. Também não andas por aí a partilhar o código do teu multibanco, pois não? Não te esqueças de alterar a palavra-passe da tua rede Wi-Fi e a chave de administração do router. Podes alterar esta última através da página web do teu administrador, na secção «Router Access».

Posso escolher quem se pode ligar à minha rede?

Se quisermos ativar este sistema de filtragem, temos de ter em conta o nosso tipo de dispositivo:

Android:
em «Definições», seleciona a opção «Wi-Fi» e depois «Definições avançadas».

iOS:
em «Definições», seleciona a opção «Geral», depois «Informações», e por último «Endereço Wi- Fi».

Windows:
aqui é um pouco mais complicado, mas se seguires bem os passos seguintes não terás problemas.
1. Vai ao botão do Windows e na caixa de pesquisa escreve «Executar».
2. Escreve «cmd» e prime Enter.
3. Na janela seguinte, escreve «ipconfig/all» e prime Enter.
4. Procura a epígrafe que diz: «endereço físico».

Mac:
em «Preferências do sistema», seleciona a opção «Redes» e depois «Airport». O sistema Mac dispõe de uma opção de filtragem através da qual escolhemos quais os dispositivos que se podem ligar à nossa rede. Isto é muito útil para evitar que alguém se aproveite da nossa ligação.

2. Protege as tuas contas com a verificação em dois passos

Protege as tuas contas com a verificação em dois passos

A verificação em dois passos consiste numa dupla proteção para as tuas contas. Isto significa que, cada vez que utilizares as tuas palavras-passe, será enviado um código para o teu telemóvel que te permitirá aceder finalmente à conta ou dispositivo em questão. Outra opção é utilizar uma chave de segurança, que deves introduzir na porta USB do teu computador quando este te pedir o código. A escolha é tua!

Como ativar a verificação em dois passos

Google
1. Inicia sessão no Google
2. Vai a «A minha conta».
3. Clica em «Iniciar sessão e segurança».
4. Introduz um número de telefone para onde enviar os códigos de acesso. Para maior segurança, marca a opção de te voltarem a pedir o código, mesmo que te ligues várias vezes a partir do mesmo dispositivo.

Microsoft
1. Inicia sessão na tua conta Microsoft
2. Na secção «Verificação em dois passos», seleciona «configurar verificação em dois passos».
3. A partir deste ponto, o procedimento é igual ao anterior. Basta seguir as instruções, como introduzir o teu número de telefone.

Apple
1. Inicia sessão na página da conta do ID Apple
2. Seleciona a opção «verificação em dois passos».
3. Clica em «Começar».
4. Responde às perguntas de segurança e segue estes passos para terminar a configuração.

Facebook
1. Inicia sessão no Facebook
2. Vai ao menu «Definições».
3. Entra em «Segurança».
4. Procura a opção «Aprovações de Acesso» e segue os passos de configuração.

Twitter
1. Inicia sessão no Twitter
2. Vai ao perfil e acede às configurações a partir do menu do canto superior direito.
3. Depois, no menu «Privacidade e segurança», procura a opção «Verificação de acesso».

WhatsApp
1. Abre a App WhatsApp no telemóvel
2. No menu situado na parte superior direita, seleciona a opção «Definições».
3. Em seguida, seleciona a opção «Conta» e «Confirmação em dois passos».
4. Depois, basta carregar em «Ativar» e introduzir um código de 6 dígitos, que será a chave para ativar a tua conta do WhatsApp em qualquer dispositivo.

3. Em busca da melhor palavra-passe

Em busca da melhor palavra-passe

Os hackers estão cada vez mais habilidosos, pelo que não existe uma palavra-passe perfeita. Mas podemos dificultar-lhes a vida! Escolhe uma palavra-passe que não seja simples e que contenha carateres muito variados.

Como criar uma palavra-passe segura

- Deve ter pelo menos 8 caracteres diferentes formados por maiúsculas, minúsculas, números e símbolos.
- Não deve ser constituída por dados pessoais como nomes de familiares ou números de telefone.
- Deve ser longa e complexa. Mas calma, não tem de fazer sentido.
- Não deve ser uma palavra, mas uma frase, cujas palavras estão separadas por espaços ou travessões.

Porquê usar palavras-passe diferentes?

Tens uma só chave para a tua casa, para o teu escritório e para o teu carro? Pois também não deves ter a mesma palavra-passe para todas as tuas contas, dispositivos ou redes sociais. Caso contrário, já sabes que se conseguirem entrar numa das tuas contas, também conseguirão aceder ao resto.

Para ter todas estas palavras-passe sob controlo, podes recorrer a um bom gestor de palavras-passe. E claro, a escolha da palavra-passe desse gestor será a mais importante, uma vez que servirá para proteger as restantes.

4. Altera a palavra-passe se a roubarem

Em caso de roubo ou perda de uma das tuas palavras-passe, é necessário alterá-la ou tentar recuperá-la o mais rápido possível. Evitarás assim que alguém faça uma utilização ilícita das tuas contas e poderás aceder às mesmas com total normalidade.

Como escolher a pergunta secreta

Já sabes que, muitas vezes, quando escolhes uma palavra-passe para uma das tuas contas, te pedem que seleciones uma pergunta secreta.

- Não forneças dados pessoais.
- O truque está em escolher uma resposta que não corresponda à pergunta (e cuidado: nem nomes, nem datas).

Esta pergunta secreta ou outra modalidade semelhante servirão para o caso de, a dada altura, teres de recorrer ao processo de recuperação de palavras-passe disponível em qualquer plataforma.