

DATA
DETOX
KIT



Linha
Internet
Segura
800 219 090

APAV®
Associação Portuguesa
de Apoio à Vítima
Apoio à Vítima



Centro
Internet
Segura

 Co-financiado pela União Europeia
O Mecanismo Inteligente a Europa



FCT
Fundação
para a Ciência
e a Tecnologia
Computação Científica Nacional
FCCN

APAV®
Associação Portuguesa
de Apoio à Vítima

altice
fundação

 Microsoft

DATA DETOX KIT



Linha
Internet
Segura
800 219 090

APAV[®]
Associação Portuguesa de Apoio à Vítima
Apoio à Vítima

Desenha a tua Selfie:

**Este Data Detox
Kit pertence a:**

**Segue este Kit e encontra
formas de proteger
os teus dados.**

Diz-nos o que pensas! Nós queremos
conhecer o feedback de crianças,
jovens, educadores e pais.
Visita datadetoxkit.org/pt/families
e descobre mais.



Um Produto de
**TACTICAL
TECH**
Versão
Portuguesa
APAV



Um Produto de

**TACTICAL
TECH**

Versão

Portuguesa

APAV

#datadetox

info@data-detox.nl



Um produto de

Tactical Tech

datadetox@tacticaltech.org

www.datadetoxkit.org

Apoiado por:

APAV - Associação Portuguesa de Apoio à Vítima

Em parceria com:

IFLA - International Federation of Library
Associations and Institutions

Save the Children

Financiado por:

União Europeia

SIDA - Swedish International
Development Cooperation Agency

Contacto:

linhainternetsegura@apav.pt

#datadetox



**Linha
Internet
Segura**
800 219 090

APAV[®]
Associação Portuguesa de Apoio à Vítima
Apoio à Vítima



É assim que eu derrubo a desinformação

Parabéns por teres chegado ao fim do kit de desintoxicação contra a desinformação. Agora relaxa e vê tudo aquilo que alcançaste neste módulo:

- Percebi como é a minha “Filter Bubble”.
- Aprendi a identificar títulos de “click bait”.
- Aprendi a importância de pensar antes de partilhar.
- Refleti sobre o modo como posso aplicar as coisas que aprendi para defender as causas em que acredito.

A Internet pode ser um espaço avassalador em termos de informação, mas se refletir um pouco antes de partilhar algo, estou a torná-la um lugar melhor.

Partilha os teus conhecimentos com familiares e amigos/as para que também eles possam tornar a Internet num espaço mais positivo.

Para mais dicas e informação,
visita **datadetoxkit.org**

PRIVACIDADE
DIGITAL

O Data Detox Kit é o guia para explorares o mundo dos teus dados online. Porque é que toda a gente está a falar deste guia? Qual o seu aspeto? Como é que funciona?

Assume o controlo dos teus dados



... eles estão a fugir

Não parece ser muito importante as empresas recolherem os teus dados. Quem é que se importa se és fã do *Baby Yoda* ou se vês mais vídeos de gatos do que de pessoas?

O problema reside na utilização que é feita dos teus dados. **Ao longo do tempo, o teu “eu online” ganha personalidade própria, tendo os seus hábitos, gostos, as suas antipatias e segredos.** Podes perder o controlo da situação e o teu “eu online” poderá ir parar a mãos alheias – empresas que fazem dinheiro com os teus dados, por exemplo.

Vamos Começar a Explorar!

1 Reorganiza as tuas Apps

As aplicações, para além de ocuparem gigabytes preciosos de espaço e gastarem a tua bateria, podem estar a recolher os teus dados - mesmo quando não as estás a utilizar. Apagar algumas dessas aplicações é uma forma rápida de reduzir a tua "Pegada Digital" e poupar a bateria do teu smartphone bem como libertares espaço. Só vantagens, não achas?

Experimenta esta atividade para verificares se és um acumulador de Apps:

Hey!

Se não tens um Smartphone junta-te a alguém que tenha um.

Em primeiro lugar, tenta adivinhar quantas aplicações tens instaladas no teu Smartphone (Não espreites!)

Agora conta quantas apps realmente tens

Pergunta a ti mesmo, de todas essas aplicações, quantas é que realmente precisas. De seguida, apaga as que não passam neste teste. Como podes fazê-lo:

Android: Definições → Apps → Selecciona a aplicação que pretendes desinstalar → Desinstala

iPhone: Pressiona com o dedo em cima da aplicação que pretendes apagar e carrega em "Apagar a Aplicação"

Dica Importante!

Se estás na dúvida relativamente a apagar uma aplicação ou não, verifica se podes aceder à mesma através do navegador da Internet.

2

Será que o teu Smartphone sabe por onde andas?

Existe um tipo de informação que é muito valiosa para quem faz a recolha dos teus dados - a tua localização! A tua geolocalização pode revelar muito acerca de ti: desde algo tão simples como a tua idade, até algo mais íntimo como quem é o/a teu/tua melhor amigo/a. Algumas aplicações poderão estar constantemente a monitorizar todos os teus passos, sem que tenhas conhecimento. Assim, podes revelar mais informação sobre ti do que a que pretendes.

Vamos analisar as Apps que tu mais utilizas. Escreve num pedaço de papel as três apps que mais utilizas:

- 1.
- 2.
- 3.

Para cada uma destas aplicações coloca a ti mesmo a seguinte questão: Esta aplicação necessita de aceder à minha localização para funcionar melhor?

Esta App precisa de ter acesso à minha localização:

Nunca

Às vezes

Sempre

Hey!

Algumas aplicações para funcionarem corretamente vão necessitar de ter acesso aos teus dados de localização, como um mapa ou uma aplicação de meteorologia:

Android: Definições → Apps → Verificar as definições de localização por aplicação

iPhone: Definições → Privacidade → Serviços de localização → Verificar as definições de localização por aplicação

Agora verifica as tuas Apps e, em todas aquelas que não necessitem de ter acesso à tua localização para funcionar, desativa as definições de localização:

As tuas aplicações já não têm acesso livre à tua localização, porque acabaste de o restringir! Agora que deste este passo podes tentar limitar o acesso à tua geolocalização em outras aplicações como os Contactos, Câmara e Microfone.

Bónus :)

4

Para apagar uma aplicação, carrega na cruzinha que aparece em cima da App.

3

Partilhar com Responsabilidade

A informação falsa pode ser partilhada de uma forma rápida. Este tipo de informação até pode estar a ser partilhada por pessoas em quem tu confias. É importante que saibas o teu papel e o efeito que pode ter a propagação de informação falsa na Internet.

Escreve a última partilha online que fizeste com uma/um amiga/o:

O que é que chamou a tua atenção?
...tinha uma imagem chocante?

Era da autoria de quem?
... que website, quem era o autor?

Porque é que partilhaste?

Pergunta a ti mesmo,
"Ao partilhar, tornei o mundo num lugar melhor?"

Sim

Não

Agora tenta responder às seguintes questões:

Onde é que viste esse conteúdo?

redes sociais
site de notícias
app de chat p. ex. WhatsApp
outro

Na tua opinião, qual o fim do conteúdo criado?

Podes seleccionar mais que um

para provocar
para inspirar
para educar
para informar
para entreter
outro

Foi difícil para ti responder a todas estas questões? Ter todos estes pontos em consideração antes de partilhar pode ser complicado, principalmente quando tens à tua frente conteúdo que te choca ou deixa maravilhado. No entanto, é importante a reflexão. Pensa duas vezes antes de partilhar.

4

Tem Consciência do teu Poder para influenciar o teu Ecosistema Digital

Nós partilhamos coisas por todos os tipos de razões – por aborrecimento, porque tem piada ou por entusiasmo; mas também porque nos preocupamos com as coisas. As causas que nos preocupam fazem parte daquilo que somos, influenciam o nosso discurso, a nossa forma de agir, com quem nos damos. O mesmo também se aplica ao que fazemos online.

Pensa num tema ou numa causa que defendas e escreve-a no espaço em branco (causas como as mudanças climáticas, feminismo, direitos dos animais, desporto, alimentação)

Agora tenta responder às seguintes questões assinalando aquelas que se aplicam a ti: Eu vi outros utilizadores/as a falarem sobre este tópico...

...partilhando artigos chocantes, embora possam não ser verdadeiros

... partilhando pensamentos como se fossem factos, apesar de se tratar apenas da opinião de quem os partilha

... partilhando imagens que parecem ser algo que na verdade não são

...seguindo uma tendência, porque é viral

Expressas ativamente as tuas causas? Muitas vezes as pessoas partilham coisas, sobre as quais não estão de acordo, para tentar provar o seu ponto de vista. Da próxima vez que verificares estar a ser disseminada informação falsa sobre um tópico com o qual te preocupas, pensa duas vezes antes de comentários, partilhares ou publicares. Ao invés, se te sentires confortável, denuncia na Plataforma com indicação de informação falsa/não-verificada.

Sabias que?

Quando, em 2019, os fogos na Amazónia começaram a deflagrar, líderes mundiais, tal como o presidente francês, partilharam imagens falsas dos fogos que circulavam na internet, sem saberem que as mesmas eram falsas

1

Estoura a tua "Filter Bubble"

Uma "filter bubble" é o conteúdo que tu vês, que é fruto de uma previsão que um algoritmo fez baseando-se nas tuas preferências. Parece-te bem? Mostrarem-te apenas conteúdo que se adequa aos teus interesses até pode ser uma boa ideia, mas por outro lado já pensaste em tudo aquilo que não estás a ver?

Primeiro, vamos pensar na informação que vês e na informação que não vês.

Junta-te com um/a amigo/a ou familiar e sigam estes passos nas vossas contas de **Instagram**:

Vão a "procura" e "explora" (segundo icone a contar da esquerda no canto inferior esquerdo)

Nota!

Para estas plataformas não é apenas considerado nas tuas preferências o conteúdo que gostas e partilhas, mas também o tempo (número de horas ou minutos) que vês determinado conteúdo.

Escreve, na bolha do lado esquerdo, as 5 coisas principais que vês e, o/a teu/tua parceiro/a, na bolha do lado direito. Caso ambos vejam conteúdo semelhante, coloquem-no na interseção da bolha esquerda com a direita:

O que vês	O que ambos veem	O que a outra pessoa vê
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.

O conteúdo na tua bolha está lá, porque o Instagram monitoriza aquilo que vês na plataforma.

Muitas vezes não consegues rebenotar a tua "Filter Bubble", mas podes aumentá-la. Gostas de algum conteúdo que o/a teu/a amigo/a gosta? Procura esse conteúdo no Instagram e vais ver que essa pesquisa vai levar a outras e aumentar a tua "Bolha".

2

Aprende a Reconhecer Quando Estás a ser "Fisgado"

"Click bait" é um termo usado para descrever títulos sensacionalistas ou falsos, cujo único objetivo é levarem-te a clicar nesses mesmos títulos. O título do artigo até parece muito interessante, mas depois quando o lês é bastante aborrecido e, no final, acabaste por nem ficar chocado, nem surpreendido, com a informação. Diz-nos quando foi a última vez que clicaste em algo deste género...

"Não vai acreditar nestes 5 truques de beleza! O número 5 é surpreendente"

"Inacreditável! Ela comeu isto diariamente e ficou assim..."

"Homem vs. Tubarão: O que vai ver a seguir vai surpreendê-lo..."

Pensa em alguém que conheces bem. Agora tenta criar o teu próprio título de "click bait" para essa pessoa. Lembra-te, tem de ser suficientemente sensacionalista para chamar a atenção da pessoa e levá-la a clicar:

TÍTULO

Embora possa parecer divertido criar títulos bizarros e chocantes, é importante que saibas que empresas e websites ganham dinheiro a criar estes títulos, levando pessoas a clicar neles e conseguindo muitas vezes a disseminação de informação e notícias falsas.

Sabias que?

As "Filter Bubbles" não existem apenas nas redes sociais. Existem também em aplicações de streaming como Netflix, ou motores de busca como o Google e plataformas de vídeo como o YouTube.

3

Quem é que o Google pensa que és?



É importante que saibas que ao utilizar produtos de forma gratuita, como alguns serviços da Google, estás constantemente a fornecer os teus dados. Desta forma, empresas como a Google podem utilizar essa informação de forma a criar o teu perfil online, o que ajuda as agências publicitárias a perceber os teus gostos. No entanto, muitas vezes, este perfil online não é o que achavas ser.

Vamos ver então qual é o perfil online que estas empresas criaram, baseando-se na tua atividade digital. Primeiro seleciona todos os produtos da Google que utilizas:

Motor de busca	Classroom
Gmail	Drive
YouTube	Hangout
Maps	Family Link

Agora explora o perfil que a Google criou acerca de ti:

Vai a myactivity.google.com → Autenticação → Outra atividade Google → Definições de anúncios → Controlar as definições de anúncios → Ver a personalização que foi feita de acordo com as tuas preferências

(Se a opção de "personalização de anúncios" estiver desativada, ativa-a apenas para esta atividade)

Estavas à espera de ver este teu "eu digital"? Se calhar enganaram-se na tua idade ou verificaste informação que dizia que gostavas de fazer bolos quando nunca fizeste nenhum na vida? Se não queres que seja criado este perfil online de acordo com as tuas preferências, **podes sempre desligar esta opção.**

Em myaccount.google.com/activitycontrols, podes desligar a monitorização da tua atividade online, histórico de localizações e histórico de Youtube.

Bónus :)

4

Quando partilhas mais do que aquilo que devias

Todos nós sabemos que as redes sociais são uma forma muito importante de nos conectarmos com os nossos amigos. No entanto, também é o local onde tendemos a revelar mais do que devíamos, acerca de nós, a estranhos, entre os quais estão, muitas vezes, as empresas que são donas destas plataformas.

Queres garantir que estás a partilhar conteúdo apenas com os/as teus/as amigos/as e seguidores/as e com mais ninguém? Escolhe uma das seguintes aplicações e vê quanto longe podes chegar:

Instagram Perfil → Definições

1. Conta → Sincronização de Contactos → Desliga a opção de sincronizar contactos
2. Conta → Associação entre contas → Retira a associação entre contas

Hey! Não podes desligar a associação entre a tua conta de Facebook e Instagram, ambas fazem parte da mesma empresa: o Facebook!

Snapchat

Perfil → Definições

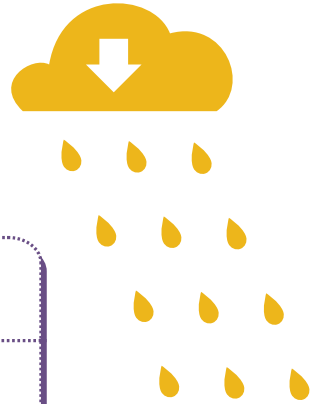
1. Serviços Adicionais → Controlo → Preferências de Publicidade → **Desativa todas as preferências de Publicidade**
2. Serviços Adicionais → Estilo de Vida & Interesses → **Desativa a opção de Estilo de Vida & Interesses**
3. Serviços Adicionais → Mapas → **Turn off Maps usage data**

Hey!

Sempre que te registares em novas aplicações, nunca o faças através do registo das tuas redes sociais. Isto permite que haja maior partilha dos teus dados entre as empresas. Ao efetuares o registo utiliza antes o teu e-mail.

Usas plataformas de Gaming como o Fortnite ou o Minecraft? Tenta reforçar as tuas definições de privacidade nessas plataformas também.

Bonus :)



A Minha Privacidade Digital

Parabéns! Acabaste de conseguir desintoxicar a tua privacidade digital. Agora relaxa e vê o que conseguiste atingir através destes diferentes passos:

- Percorreste as tuas aplicações, e livraste-te dos seus localizadores.
- Limpaste os teus dados de Geolocalização.
- Olhaste para ti através dos olhos da Google.
- Ganhaste o controlo daquilo que partilhas nas tuas redes sociais.

Mesmo que tenhas feito apenas uma destas coisas já fizeste progressos no que à tua privacidade online diz respeito. Viver num mundo em que os dados e a informação são dominantes requer a sua prática. Com o tempo, vais conseguir salvaguardar a tua informação sem esforço.

Espalha a Palavra! Encoraja os teus familiares e amigos/as a desintoxicarem os seus dados também!

De seguida:
Segurança Digital

DESINFORMAÇÃO

A Arte Marcial da Desinformação

...corta com o caos

A internet é um mar de informação – uma rede gigantesca de histórias, notícias sobre celebridades e políticos, anúncios que tentam vender-te o último modelo de ténis. Onde lês opiniões sobre TUDO e tens milhões de memes de animais. Tem tanto para oferecer!

Muitas vezes é difícil distinguir o que é verdadeiro do que é falso e de tudo o que está pelo meio.

Neste módulo, **vais aprender a importância de partilhar com consciência.**

Vamos começar!





O meu Bem-Estar Digital

Parabéns, chegaste ao fim da tua desintoxicação de Bem-Estar Digital! Agora descontraí, relaxa e confere tudo o que conseguiste fazer:

- Identifiquei o que gosto e o que não gosto relativamente ao uso da tecnologia.
- Reconheci alguns padrões de design nas aplicações que uso.
- Aprendi a desligar algumas dessas características/funcionalidades de design.
- Encontrei a minha própria forma de ter uma relação mais equilibrada com a tecnologia.

Ser inteligente com o smartphone não significa atirar o telemóvel para um rio, significa encontrar uma forma de desfrutar da tecnologia sem que ela assuma o controlo da tua vida. **Vê se podes partilhar** algumas destas técnicas de bem-estar digital com os teus familiares e amigos/as.



**Seguinte:
Desinformação**

Reforça a tua Cibersegurança

... Com palavras-passe fortes



Se a internet fosse apenas um lugar para partilhar fotos de cães mascarados de dinossauros, não haveria muita necessidade de segurança. No entanto, a internet é um local onde passas muito do teu tempo, por isso deves tornar as tuas contas **seguras**.

Aqui está uma forma de verificares se as tuas contas são seguras: estás a utilizar o nome do teu animal de estimação como palavra-passe? Hoje em dia não existem desculpas para teres uma palavra-passe fraca. À medida que os Hackers melhoram os seus ataques informáticos para terem acesso aos teus dados pessoais, deves acompanhar essa tendência e garantir que eles não acedem às tuas contas.

Ao acompanhares este Data Detox, **vais aprender a melhor maneira de criares senhas fortes e seguras, que mantêm as tuas contas protegidas de estranhos.**

Vamos começar!



1

Como ficar amigo/a de um/a Hacker

Existe uma forma muito fácil de fazeres amizade com um hacker – criares palavras-passe fáceis de descodificar, para que se sintam bem-vindos.

Tenta adivinhar as 6 passwords mais utilizadas, usando as seguintes pistas:

1. **Conta até seis (em números)**

2. **Vais precisar dela para desbloquear a tua conta**

3. **As primeiras teclas de um teclado soletram esta palavra de seis letras**

4. **Vou ao procurar a resposta (motor de busca mais popular)**

5. **Um animal que balança das árvores e come bananas**

6. **Convida um Hacker e faz com que se sintam ...**

(1) 123456 (2) senha (3) qwerty (4) google (5) macaco (6) bem-vindo

Foi fácil descobrires as respostas, não foi? Se foi fácil para ti, também é muito fácil para outras pessoas descobrirem estas palavras-passe.

É muito comum escolhermos palavras-passe que sejam fáceis de lembrar e relacionadas com algo pessoal. Desta forma, alguém que tente invadir a tua conta pode fazê-lo facilmente apenas com alguns palpites ou executando programas que permitam descodificar as palavras-passe menos complexas.

Bonus :)

Podes facilmente verificar se a tua conta de e-mail esteve envolvida numa violação de dados, através do site <https://haveibeenpwned.com/>. Se vires que a tua conta foi alvo de um ataque informático, é uma boa altura para alterares as tuas palavras-passe por outras mais seguras

2

Adeus, '123456'



Criar uma palavra-passe (password) forte é fácil. Tudo o que tens a fazer é seguir alguns princípios básicos.

A tua password deve ser:

Extensa as palavras-passe devem ter no mínimo 8 caracteres. Melhor ainda? 16-20 caracteres.

Única cada password que utilizas – para cada website – deve ser diferente.

Aleatória a tua password não deve seguir um padrão lógico ou ser fácil de adivinhar.

Segura coloca as tuas passwords num local seguro; não as escrevas num local onde qualquer pessoa as encontre.

Privada não partilhes as tuas palavras-passe com ninguém, a não ser que seja alguém que ajude a gerir as tuas contas na internet (ex. pais).

Se te parece difícil criares uma password forte, ainda mais difícil deve ser guardar essas palavras-passe, não achas? Um gestor de palavras-passe como as aplicações **1Password** ou **KeePassXC**, geram as passwords por ti de forma aleatória e guardam todas as tuas passwords em segurança. Só precisas de te lembrar de uma palavra-passe mestre para desbloquear as restantes – o teu trabalho fica mais facilitado!

Sabias que?

Um computador levará em média cerca de 7,5 milhões de anos a descodificar uma password de 12 caracteres comparado com uma password de 8 caracteres que, em média, será descodificada em 2,6 dias.

3

Mantém alguma Distância

Se o design das aplicações foi feito para te atrair, o que é que podes fazer quanto a isso? O lado positivo é que a maioria das plataformas está a tornar mais fácil vencer estes truques de design, seja através de lembretes que te avisam quando estás a passar demasiado tempo online – o Instagram já tem essa funcionalidade, mas cada vez mais apps monitorizam o tempo médio que passas no ecrã, basta que faças uma simples alteração nas definições

Aqui estão algumas coisas que podes fazer:



WhatsApp

Definições → Conta
→ Privacidade →
Recibos de Leitura →
Desligar

YouTube

Reprodução Automática
Autoplay → Desligar

Instagram

Perfil → Definições →
A tua atividade →
Definições de notificações
→ Desligar

TikTok

Perfil → Definições e Privacidade →
Bem-Estar Digital → Gestão do tempo
de ecrã → definir o tempo máximo
de utilização

Lembra-te que estas definições não têm de ser mudadas para sempre. O truque é ultrapassar a vontade urgente de verificar o telemóvel a cada minuto. Quando as voltares a ligar, podes perceber como eram irritantes e talvez voltes a desligá-las.

4

Dá-lhe uma nova oportunidade

Se queres que a tua relação com o teu telemóvel/tablet funcione, tem de ser nos teus termos. Volta ao primeiro exercício e vê os pontos positivos que indicaste acerca da utilização das tecnologias. Pode ser muito bom, certo? O truque está em desfrutares do tempo que passas online.

Escolhe as tuas próprias estratégias. Aqui tens algumas que podem ajudar:

Coloca o teu smartphone virado para baixo, ou ainda melhor, coloca-o onde não o consigas ver.

Coloca o smartphone temporariamente em silêncio ou desliga as notificações.

Se as pessoas ficarem chateadas por estares ao telemóvel, explica-lhes o que estás a fazer (lembra-te que para quem vê, parece que estás apenas a olhar para um ecrã).

Sentes-te tentado a pegar no teu smartphone? Pergunta a ti próprio porquê.

Verifica as tuas estatísticas de tempo de utilização – desafia-te a ti e aos/às teus/tuas amigos/as a reduzir esses tempos.

Bonus :)

Consegues pensar em mais estratégias para diminuir o tempo de utilização?

LIFEHACK

Nota!

Se já usas algumas destas estratégias, retira-as da lista!

1

Pensa nos bons tempos

Podemos ter uma relação de amor-ódio com a tecnologia. Ao mesmo tempo que a tecnologia nos permite socializar e comunicar com amigos, também é a tecnologia que nos poderá levar a sentirmo-nos sozinhos, ou com medo de estar a perder alguma coisa (FOMO).

Quando estás na internet o que é que fazes mais? (jogos online, conversar com amigos, ver televisão?).
Escreve na tabela do meio o que fazes mais na internet. Agora, na tabela da esquerda, escreve o que aprecias mais nessa atividade e, na da direita, o que gostas menos nessa atividade.

Gosto

Na internet passo mais tempo a

Não Gosto

Bónus :)

Achas que podes riscar alguma coisa da coluna "Não Gosto" até ao final deste Data Detox? Pensa em como podes obter um equilíbrio para que possas tirar o máximo partido da utilização do teu dispositivo.

2

Lembra-te: A Culpa Não é Tua

Podes sentir-te como se toda a gente dissesse a ti e aos/às teus/tuas amigos/as para não estarem tanto tempo ao telemóvel. Mas alguma vez pensaste que pode não ser culpa tua estares tão dependente do telemóvel? Torna-se intuitivo deslizar, gostar e partilhar. Certas características do design das aplicações são muitas as culpadas por passarmos tanto tempo online.

Tenta combinar as características de design à esquerda com as aplicações abaixo.

●●● **Bolha da escrita** - aqueles três pontos que indicam que alguém está a escrever uma mensagem. Oh, o suspense!

A tendência - uma nova dança, meme ou estilo que aparece em todo o teu feed

▶ **Reprodução automática** - Não é preciso clicares, o próximo vídeo vai surgir em 3, 2, 1...

∞ **O toque infinito** - conteúdo que continua a surgir

👤 **A loot box** - prémios de jogos ou moedas que podem ser resgatados para obtenção de mais bens

♥ **O gosto** - o polegar para cima ou coração que permitem reconhecimento (gostar de algo)

★ **A winning streak** - a recompensa pela lealdade; quando se perde tens de recomeçar tudo

🔄 **Puxar para atualizar** - aquele lapso de tempo que cria suspense enquanto esperas por carregar mais conteúdo

Nota!

Podes concluir que certas funcionalidades de design são encontradas em mais do que uma aplicação.

Sabias que?

Em média, uma pessoa comum clica, toca e desliza 2.600 vezes por dia no seu telemóvel? E tu, quantas vezes o fazes por dia?

1. YouTube
2. TikTok
3. Snapchat
4. Fortnite
5. Instagram
6. Netflix
7. Spotify
8. WhatsApp

3

PrEGuiças S@Itam de forma selvagem! NO Sup3rMercado

Porque é que, de repente, estamos a falar de preguiças? O tema deste capítulo são as palavras-passe em forma de frase (passphrase) Uma cadeia aleatória de palavras tão estranhas que, na verdade, se tornam mais fáceis de lembrar do que uma senha, mas muito mais difíceis de adivinhar por um intruso.

Tenta agora criar a tua própria palavra-passe em forma de frase. Escreve 5 palavras aleatórias, de forma a criares uma frase estranha como a que está no título deste capítulo:

1	2	3	4	5
---	---	---	---	---

Agora, de forma aleatória, coloca algumas das letras em MAIÚSCULO, acrescenta alguma pontuação (!?) e números e reescreve a frase abaixo:

1	2	3	4	5
---	---	---	---	---

Parabéns, acabaste de criar a tua passphrase!

Para a maioria dos humanos é muito difícil decorar combinações aleatórias de letras e números (passwords), mas torna-se mais fácil memorizar frases e palavras (passphrases).

Nota!

Lembra-te que não debes guardar as tuas palavras-passe onde alguém as consiga encontrar. Isso significa que não podes usar a frase do exercício, mas agora sabes como criar uma e como guardá-la num lugar seguro, ou num lugar onde possas facilmente apagar os vestígios.

4

Dá duas voltas à fechadura da tua porta digital

Se seguiste todos os passos acima, debes ter dificultado a invasão da tua conta por alguém (hacker). Mesmo assim, palavras-passe super fortes não são invencíveis.

A autenticação de dois fatores (2FA) ou autenticação de múltiplos fatores (MFA) é basicamente uma camada de segurança extra que impede alguém de entrar na tua conta, mesmo que conheça a tua palavra-passe – pensa nisso como colocar uma segunda fechadura na tua porta. A maioria das aplicações fornece esta camada extra de proteção.

Tenta ativar esta opção, nas tuas aplicações:

Instagram:

Perfi → Definições
→ Segurança →
Autenticação de 2-fatores
→ Começar

Snapchat:

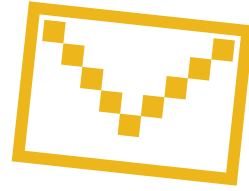
Definições →
Autenticação de 2-fatores

Google:

Acede a <https://myaccount.google.com> →
Segurança → Autenticação na conta Google →
Verificação de 2-passos

Nota!

A autenticação de 2-fatores permite que utilizes a tua conta de e-mail ou uma senha de uso único como segundo fator de autenticação, em vez de associares um número de telemóvel. Desta forma mesmo que deixes cair o teu telemóvel na sanita, vais conseguir aceder às tuas contas.



A Minha Segurança Digital

Parabéns! Chegaste ao final da sessão - como desintoxicar a tua segurança digital. Agora relaxa e vê tudo o que conseguiste alcançar:


- Já sei que palavras-passe não devo utilizar.
- Aprendi os 5 princípios para ter uma password forte e segura.
- Criei a minha palavra-passe em forma de frase.
- Consigo ativar a autenticação de 2-fatores em, pelo menos, uma conta.

Agora que já te sabes defender de ataques às tuas contas partilha estes conhecimentos com a tua família e amigos/as. Os teus familiares e amigos/as irão agradecer-te, pois também eles poderão “navegar” com maior segurança.

**A seguir:
Bem-Estar
Digital**

Como Sobreviver a uma Separação

...com o teu Smartphone



Já deste por ti a olhar para o ecrã do teu smartphone, sem perceberes bem como é que isso aconteceu? Ou talvez tenhas ido ver alguma coisa ao telemóvel e, de repente, BAM! Passaste uma hora a fazer “scrolling” no INSTAGRAM?

As nossas relações com a tecnologia podem exigir muito de nós, especialmente com todos os buzzes, pings, luzes e alertas que recebemos. Às vezes é difícil lembrarmo-nos do porquê de gostarmos de ter um telemóvel connosco.

À medida que vais seguindo este guia, vais aprender a estabelecer um melhor relacionamento com os teus dispositivos eletrónicos.

Vamos começar!

