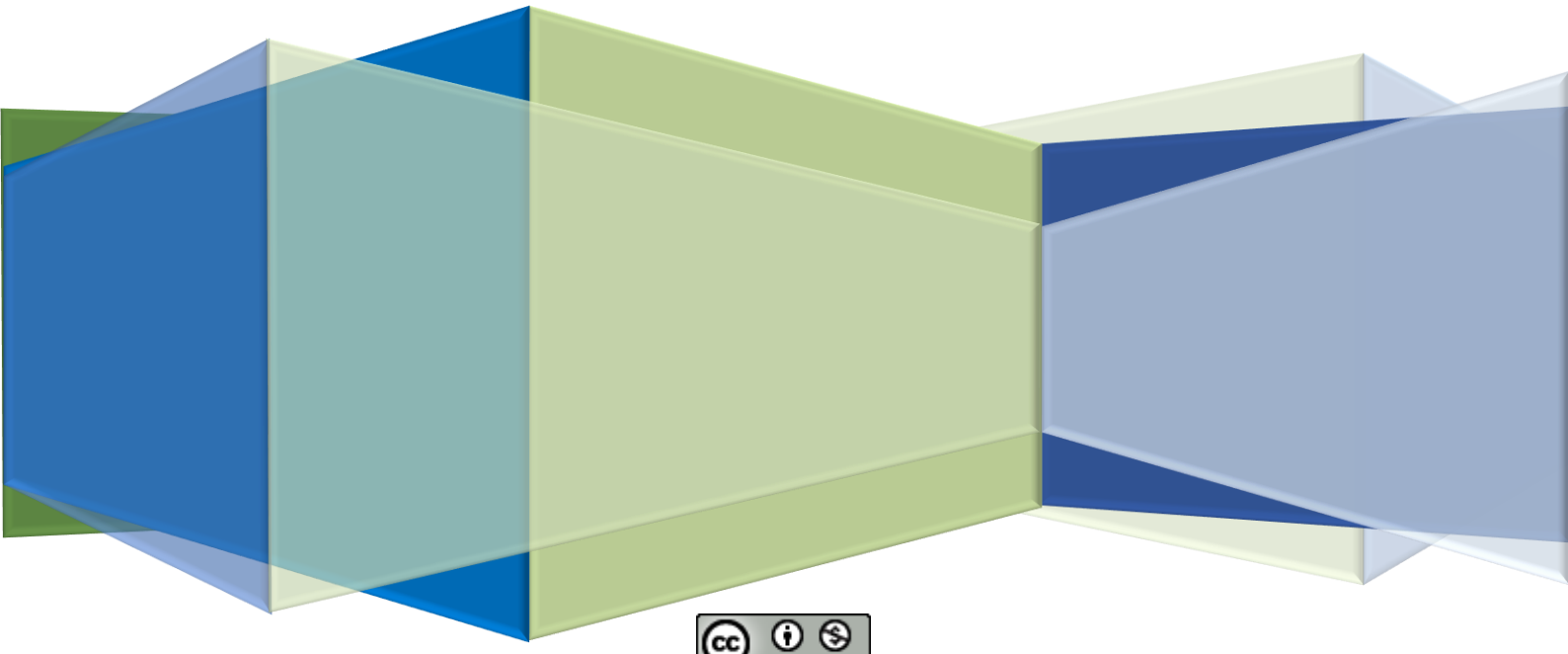
Agrupamento de Escolas de Paços de Brandão

Manual de boas práticas digitais

Volume 2 – Segurança Digital



Uma escola com vida e para a vida!

Segurança Digital

No mundo digital todos devemos ter hábitos e comportamentos ciberseguros, incutindo desde cedo às nossas crianças e jovens um conjunto de regras a cumprir no espaço digital, visto que a segurança online está em pequenos gestos do nosso dia-a-dia.

Usar palavras-passe fortes

Uma palavra-passe ou *password* é a nossa chave para entrar em contas online. Ela é como a nossa escova de dentes: não se partilha com ninguém e deve ser trocada regularmente.

Para criar uma **palavra-passe segura** devemos seguir as seguintes regras:

- usar pelo menos 8 caracteres;
- usar letras maiúsculas, letras minúsculas, números e símbolos;
- não usar o nome de utilizador, data de nascimento, telemóvel ou outro dado pessoal;
- não usar conjuntos de dígitos consecutivos ou que se encontrem juntos no teclado;
- usar palavras-passe diferentes para sites diferentes;
- nunca guardar as palavra-passe no *browser* dado que há *malwares* que roubam as credenciais memorizadas nos *browsers.*

Mas não é suficiente criar apenas uma palavras-passe forte, é necessário alterar as mesmas com frequência e recorrer à autenticação de duplo fator, procedimento recorrente por instituições bancárias, comércio eletrónico e e-mail.

Nunca devemos usar a mesma palavra-passe em sites diferentes.

Se alguém descobrir essa palavra-passe, facilmente entrará em todas as contas online.

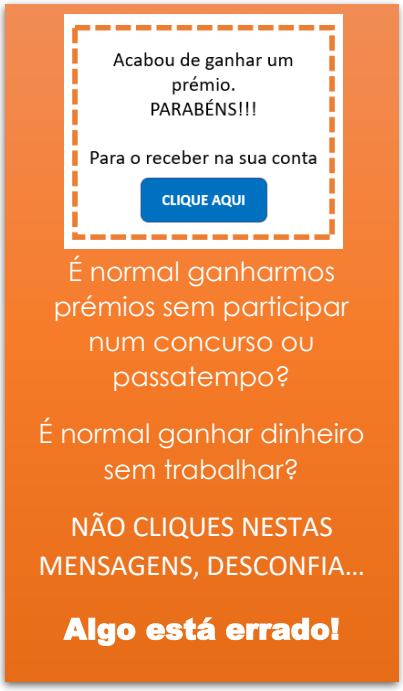
Estar atento a *Malware* e *Phishing*

Malware é software malicioso criado com o intuito de destruir ou recolher informações do dispositivo eletrónico, podendo mesmo controlá-lo. Há várias tipologias de *malware*, por exemplo, um vírus informático que muitas vezes instala-se automaticamente no computador e cria dificuldades de funcionamento do dispositivo. É fácil um vírus entrar no nosso sistema, através de anexos de e-mails, quando descarregamos programas, músicas, imagens, vídeos ou até quando acedemos a sites.

Atualmente é recorrente ouvir falar de **esquemas de *phishing***, uma armadilha onde as pessoas são enganadas, visto que o atacante faz-se passar por uma empresa credível através de sites, SMS ou e-mails falsos. Podem solicitar a confirmação de dados pessoais ou incitam a clicar em links, pedem falsos donativos ou falsas ofertas de comércio eletrónico. Estes esquemas são cada vez mais rebuscados, necessitando o utilizador de estar atento para determinados aspetos.

Como proteger de *malware* e esquemas de *phishing*?

- Não divulgar dados pessoais como o nome, morada, contato, idade na Internet, por exemplo, nas redes sociais.
- Verificar o URL do site onde se insere informações pessoais.
- Ter cuidado com os links a que se acede em mensagens instantâneas, e-mails ou sites, refletir se faz sentido o que estão a solicitar.
- Verificar se o endereço dos sites é o original e confirmar se o mesmo possui uma navegação segura (símbolo 🔒 ou https).
- Antes de abrir e executar um ficheiro verificar a existência de vírus.
- Descarregar aplicações apenas de fontes seguras, como o site oficial do proprietário.
- Manter todo o tipo de software do computador ou dispositivo eletrónico sempre atualizado.
- Instalar um antivírus mantendo-o atualizado.
- Nunca desativar a firewall do sistema operativo do dispositivo eletrónico.
- Usar mais do que uma palavra-passe para sites diferentes.



Proteger o nosso equipamento

Manter o nosso equipamento seguro (computador, tablet, telemóvel…) é a primeira etapa de defesa em questões de segurança digital. Se em nossa casa implementamos mecanismos para proteger os nossos bens, no nosso dispositivo eletrónico também devemos seguir as principais recomendações:

- Manter o sistema operativo sempre atualizado, bem como todo o software de aplicação;
- Instalar um antivírus mantendo-o atualizado;
- Nunca desativar a firewall do sistema operativo do equipamento;
- Descarregar e instalar aplicações de sites ou lojas oficiais.
- Cobrir com fita adesiva a câmara do dispositivo quando não estiver a ser utilizada evitando que a mesma esteja a ser acedida remotamente.

… ainda nos dispositivos móveis:

- Bloquear o dispositivo com senhas fortes ou dados biométricos;
- Cuidado com as autorizações cedidas às apps, dar permissão do estritamente necessário para a aplicação funcionar;
- Em ambientes públicos, desativar *Bluetooth* e *Wi-fi* quando não se estiver a utilizar.

Fazer cópias de segurança

Para proteger os nossos dados existentes no computador ou noutros dispositivos eletrónicos é muito importante efetuar **cópias de segurança** (***backup***) frequentemente, evitando perder a informação em situações de avaria do dispositivo, infeção por vírus ou bloqueado por *ransomware*.

As cópias de segurança podem ser feitas para uma *pendrive*, disco externo ou para um serviço de armazenamento online (Google Drive, OneDrive, MeoCloud…).

Proteger a nossa privacidade

Nunca foi tão fácil partilhar informação, já não sabemos viver sem a Internet sendo fundamental salvaguardar a privacidade dos nossos dados pessoais. Com as redes socias, as lojas online e outras plataformas de partilha de informação aumentou o risco de violação da nossa privacidade, sendo importante adotar comportamentos para protegê-la:

«APRENDER COM CONFIANÇA PARA NAVEGAR EM SEGURANÇA!» NUNCA DÊS OS TEUS DADOS PESSOAIS: NÃO DIGAS EM QUE ESCOLA ANDAS, TEU NÚMERO DE TELEFONE, A TUA MORADA, NEM MESMO O TEU NOME VERDADEIRO!

Fonte: Internet Segura (2022). *ZIGZAGA NA NET.*

- Não divulgar os dados pessoais nas redes sociais, nem registar em janelas de pop-up.
- Não publicar fotografias que identifiquem o local de residência/escola.
- Pedir autorização aos intervenientes presentes em fotografias ou vídeos quando se publica este tipo de informação nas redes sociais ou em outros *sites*.
- Pensar bem antes de publicar, depois de publicado um conteúdo dificilmente pode ser retirado da Internet.
- Evitar a utilização de redes públicas.
- Usar o modo de navegação anónima, quando o computador é público.
- Manter todo o software do computador devidamente atualizado.
- Usar palavras-passe fortes e seguras, alterá-las com regularidade e não as guardar nos *browsers*.

Dicas a seguir nas redes sociais

Uma rede social não é um diário.	Cuidado com as fotografias, vídeos, comentários publicados.	Manter o perfil privado.
Cuidado com os encontros.	Não responder a mensagens, nem aceitar pedidos de desconhecidos.	Não partilhar informação pessoal.

Identificar notícias falsas

Diariamente somos confrontados com notícias através das redes sociais ou em *sites* que nem sempre são verdadeiras, conhecidas por *fake news.* Estas notícias são criadas com o objetivo de gerar algum tipo de benefício (económico, social, político) espalhando boatos e mentiras que prejudicam pessoas, empresas, políticos e figuras públicas.

As notícias falsas normalmente são apelativas, sensacionalistas, cheias de emoção, sendo facilmente partilhadas através das redes sociais, aplicações de mensagens e por vezes escondem *malware*.

Para identificares notícias falsas segue as seguintes dicas:

- **Verifica a sua origem/fonte**, tentando perceber quem a escreveu e se a pessoa ou entidade é especialista no assunto partilhado.
- Desenvolve o teu **espírito crítico**, não acredites em tudo, lê toda a notícia, as *fake news* têm títulos sensacionalistas, usam letras maiúsculas e pontos de exclamação.
- **Verifica a data da notícia**, esta pode ser muito antiga e descontextualizada da realidade atual.
- Verifica se a notícia tem a **identificação do autor** e analisa se ele existe mesmo e é confiável.
- Partilha apenas conteúdos de fontes fidedignas ou os quais sabes que são verdadeiros.
- Analisa o URL do *site*.

"Os autores de notícias falsas usam os utilizadores da Internet para disseminar mentiras e ódio. Sem os teus cliques, a tua voz, as tuas partilhas, as *fake news* ficam rapidamente offline… Procura factos, denuncia, promove os direitos humanos online porque tu podes fazer a diferença".

Fonte: IPDJ IP. Internet Segura | Discurso de Ódio - Processar Informação Forma Crítica disponível em https://www.youtube.com/watch?v=qt88y_a8zy0&list=PLMPW21PmpRYkmF_79oizf7L4WrNmjKQQO&index=7 acedido a 23-3-2022.

Combater o *cyberbullying*

O *cyberbullying* traduz-se pelo ato de exercer violência usando as tecnologias e a Internet, recorrendo às redes socias, blogues, mensageiros instantâneos, etc. Este fenómeno manifesta-se de diferentes formas: pela publicação não autorizada de fotografias, roubo de identidade, intimação, insultos através de mensagens, etc.

As crianças e jovens vítimas de cyberbullying devem:

- Se alguém te provocar ou a tentar humilhar, não respondas, ao reagires o agressor vai perceber que está a conseguir o efeito que pretendia sobre ti. Mantem-te calmo e bloqueia o agressor das tuas redes sociais e outros canais de comunicação online;
- Guarda registos do que aconteceu, através de capturas de ecrã ou gravações de conversas. Poderás, mais tarde utilizá-las para denunciar os agressores;
- Não compactues com os agressores. Quanto mais seguidores essa pessoa possuir, mais poder lhe estão a dar para magoar mais vítimas. Se estiveres a passar por alguma situação destas, recorda-te que podes entrar em contacto com a Linha Internet Segura;
- Se fores vítima de Cyberbullying pode ajuda. Procura um adulto em quem confies para denunciar ou intervir na situação.

Linha Internet Segura

800 21 90 90

linhainternetsegura@apav.pt

Fonte: Internet Segura (2019). *DICA: Como minimizar o impacto do Cyberbullying.* [online] https://www.internetsegura.pt/noticias/dica-como-minimizar-o-impacto-do-cyberbullying acedido a 12-3-2022

Estar seguro online só depende de ti, do teu conhecimento e da tua atitude. Para treinares as tuas aprendizagens sobre cibersegurança podes jogar:

Cibercidadão - SNAKES AND LADDERS

Seguranet – Jogos 1.º e 2.º ciclos

Seguranet – Jogos 3.º ciclo

Space Shelter

Interland

Referências bibliográficas

Fundação, A., s.d. *Fake News.* [Online]
Available at: https://www.internetsegura.pt/sites/default/files/2021-07/fakenews_0.pdf
[Acedido em 18 março 2022].

Fundação, A., s.d. *Privacidade na Internet Redes Sociais.* [Online]
Available at: https://www.internetsegura.pt/sites/default/files/2021-02/RedesSociais_PrivacidadeDeDadosPessoais_0.pdf
[Acedido em 20 março 2022].

Microsoft, s.d. *Proteger a sua privacidade na Internet.* [Online]
Available at: https://support.microsoft.com/pt-pt/windows/proteger-a-sua-privacidade-na-internet-ffe36513-e208-7532-6f95-a3b1c8760dfa
[Acedido em 21 março 2022].

Nunes, P., Alves, M. C. & Neto, C., 2021. *Enter 7.* s.l.:Porto Editora.

Segura, C. I., s.d. *DICA: Como minimizar o impacto do Cyberbullying.* [Online]
Available at: https://www.internetsegura.pt/noticias/dica-como-minimizar-o-impacto-do-cyberbullying
[Acedido em 12 março 2022].

Segura, C. I., s.d. *ZIGZAGA NA NET.* [Online]
Available at: https://www.internetsegura.pt/sites/default/files/2022-02/Livro%20ZigZaga%20na%20Net.pdf

SeguraNet, C. d. S., s.d. *Tiras BD SeguraNet.* [Online]
Available at: https://www.seguranet.pt/pt/tiras-bd-seguranet
[Acedido em 12 março 2022].

Tavares, A. P., Roque, E. & Xambre, L., 2021. *TecnIC.* s.l.:Raiz Editora.