CIBERSEGURANÇA

Vivemos numa era digital onde a tecnologia faz parte do quotidiano. Desde o trabalho e estudo até ao entretenimento e relações sociais, passamos muito tempo online. Apesar dos benefícios que a internet oferece, também existem riscos que devemos conhecer.

A cibersegurança é a forma de nos protegermos dessas ameaças, e garantir uma experiência segura online.

O que é e para que serve a cibersegurança?
Consiste num conjunto de práticas, tecnologias e processos para proteger os computadores, redes, sistemas e dados contra os ataques ou acessos não autorizados.
Permite proteger as nossas informações pessoais e garantir a segurança enquanto navegamos na internet. Evita que outras pessoas tenham acesso ou roubem os nossos dados pessoais como palavras-passe, fotografias, entre outros.

Riscos e Comportamentos Online
Existem vários perigos quando navegamos na internet, tais como:

- *Cyberbullying* (*bullying* na internet);
- Discursos de ódio online;
- *Grooming*/aliciamento online (manipulação psicológica/emocional envolvendo menores de idade);
- *Phubbing* (ignorar pessoas em situações sociais pela utilização de tecnologia por largos períodos de tempo);
- *Phishing* (fraude com vista a que as pessoas revelem informações pessoais como senhas, números de cartão de crédito ou outras informações financeiras);
- Roubo de identidade online;
- *Sexting* (troca de mensagens eróticas com ou sem fotos, via telemóvel, chats ou redes sociais);
- *Sextortion* (forma de exploração sexual que usa formas não físicas de coação para extorquir favores sexuais à vítima).

Ameaças e Fragilidades Digitais

- Vírus;
- *Malware* (*software* destinado a infiltrar-se em dispositivos de forma ilícita, com a intenção de causar danos, alterações e/ou roubo de informação);
- *Spyware* (tipo de *Malware* que recolhe informações sobre o utilizador, muitas vezes associada à sua atividade online, mas também informações como dados bancários e documentos confidenciais);

São algumas das ameaças que podem tornar a utilização dos diferentes equipamentos e tecnologias digitais mais vulneráveis.

Dicas práticas de Cibersegurança para Cuidadores e Crianças/Jovens:

- Usem **palavras-passe fortes** (combinem letras maiúsculas, minúsculas, números e símbolos para serem difíceis de adivinhar) e evitem voltar a usar as mesmas palavras-passe;
- Mantenham as **configurações de privacidade** nas redes sociais (não partilhem informações pessoais como, por exemplo, morada, número de telemóvel ou nome da escola);
- **Não aceitem pedidos de desconhecidos** online nem partilhem informações;
- **Atenção às fraudes:** não cliquem em *links* suspeitos nem descarreguem anexos enviados por fontes desconhecidas - podem ser vírus ou tentativas de *phishing*;
- **Atualizem regularmente o *software*** dos dispositivos;
- Utilizem **redes Wi-Fi seguras** e não acedam a informações pessoais quando estiverem a utilizar redes públicas, uma vez que nestas a segurança pode estar comprometida.

O que é e para que serve a parentalidade digital?

São medidas que os pais, cuidadores, familiares e professores devem ter em relação à utilização da internet pelos mais novos.

Permite que as crianças desfrutem dos benefícios da tecnologia enquanto são protegidas de possíveis riscos associados ao uso irresponsável e à exposição de conteúdos inadequados.

Dicas de Parentalidade Digital:

- **Converse** de forma calma e clara com o jovem, sem o julgar ou criticar;
- **Esteja** disponível para ouvir e conversar sobre dúvidas e/ou situações desagradáveis ou estranhas que se passaram na internet;
- **Participe nas atividades online** do jovem, com foco nos seus interesses/interações, e mantenha-se atualizado face às tendências digitais;
- **Defina e explique** quais são os **direitos, regras/deveres e limites** relativos ao uso da internet e dos dispositivos eletrónicos que o jovem deverá cumprir;
- **Mostre e partilhe conteúdos/sites educativos e saudáveis** (saiba mais sobre estes conteúdos na plataforma *Better Internet for Kids*);
- **Avalie** sempre as classificações de uma aplicação, jogo ou conteúdo online, bem como se são adequados à idade e ao desenvolvimento da criança/jovem;
- Utilize **ferramentas de controlo parental** (*software* específico para controlar os conteúdos visualizados, horários e os programas cujo acesso é permitido);
- Mantenha-se informado sobre cibersegurança e esclareça as suas dúvidas através da Linha Internet Segura.

Referências bibliográficas:

1. *Better Internet for Kids* [sítio na Internet, consultado 2024 out 07]. Disponível em: https://www.betterinternetforkids.eu/

2. Centro Internet Segura [sítio na Internet, consultado 2024 out 07]. Disponível em: https://www.internetsegura.pt/
3. CNCS - Centro Nacional de Cibersegurança Portugal [sítio na Internet, consultado 2024 out 07]. Disponível em: https://www.cncs.gov.pt/
4. *Social Media and Teens: The Ultimate Guide to Keeping Kids Safe Online* [sítio na Internet]. *Educate Empower Kids*. [consultado 2024 out 10]. Disponível em: https://educateempowerkids.org/wp-content/uploads/2018/05/Social_Media_Guide_Contract_Single_Pages.pdf
5. UNICEF - Segurança Digital [sítio na Internet, consultado 2024 out 29]. Disponível em: https://www.unicef.pt/seguranca-digital/

Elaborado por:
Inês Filipa Mendes e Joana Victor Lage
Internas de Formação Específica de Pediatria, Serviço de Pediatria, Hospital Professor Doutor Fernando Fonseca, Unidade Local de Saúde Amadora / Sintra

Orientado por:
Carlos Escobar, Helena Almeida e Maria de Lurdes Torre
Assistentes Hospitalares de Pediatria, Serviço de Pediatria, Hospital Professor Doutor Fernando Fonseca, Unidade Local de Saúde Amadora / Sintra

Texto elaborado para o Portal C&F, SPP 11/2024©