**Este verão, proteja-se com mais do que protetor solar**

Sete dicas da Fortinet para não deixar a sua segurança de férias

O [Relatório Global sobre o Panorama de Ameaças 2025](https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks) da **FortiGuard Labs** revelou um crescimento sem precedentes nos ataques automatizados e a proliferação de ferramentas de cibercrime com recurso a inteligência artificial. Com o verão à porta e os dispositivos móveis permanentemente ligados — entre as redes públicas de Wifi, as reservas de última hora, as ofertas imperdíveis ou as inúmeras partilhas nas redes sociais — a superfície de ataque nunca foi tão grande como agora.

*“Os cibercriminosos estão cada vez mais organizados, utilizam IA para automatizar ataques e estão a explorar o aumento da utilização digital nas férias. A verdade é que a cibersegurança não deve, nem pode tirar férias.” refere* **Rui Branco Manager Systems Engineering da Fortinet Portugal**

Para garantir que as férias não se transformam num pesadelo digital, a Fortinet partilha sete conselhos simples, mas valiosos, para levar a cibersegurança na sua bagagem.

**Sete Dicas Fortinet para um Verão Ciberseguro**

**1. Confirme a ligação Wi-Fi antes de se ligar**

Evite utilizar redes públicas de WIFI, seja em aeroportos, esplanadas ou eventos, os pontos de acesso falsos são cada vez mais comuns. Verifique sempre o nome da rede com o estabelecimento e privilegie ligações VPN para proteger as suas comunicações.

**2. Atualize tudo antes de partir**

Dispositivos e aplicações desatualizados são alvos fáceis. Os ataques mais eficazes exploram falhas conhecidas e não corrigidas. Atualize os seus sistemas antes de viajar. Garanta também uma cópia de segurança dos dados mais importantes

**3. Redobre a vigilância contra phishing**

Os ataques por email ou SMS estão a tornar-se cada vez mais convincentes, com IA a gerar mensagens quase perfeitas e impercetíveis. Desconfie de ofertas imperdíveis e links urgentes para entregas de encomendas.

**4. Use autenticação multifator em tudo**

Sempre que possível, ative a verificação em dois passos. Mesmo que a sua password seja comprometida, os atacantes não conseguirão aceder à conta sem o segundo fator. Ative também o bloqueio por PIN, impressão digital ou reconhecimento facial nos seus dispositivos

**5. Reduza as partilhas nas redes sociais**

Evite publicar que está de férias ou partilhar a sua localização em tempo real. Está a dar pistas preciosas a quem o quiser atacar — no mundo digital ou físico.

**6. Crie passwords à prova de verão**

Nada de “verao2025” ou “password123”. Aposte em frases personalizadas, com substituições criativas e diferentes para cada serviço. Utilize um password manager para facilitar a gestão de todas estas passwords

**7. Ensine os mais novos a protegerem-se online**

Com mais tempo livre e acesso a dispositivos, as crianças tornam-se alvos fáceis. Aposte em formação simples e controlos parentais. A segurança começa em casa e em cada um de nós.