SEGURANÇA EM TEMPOS DE CRISE

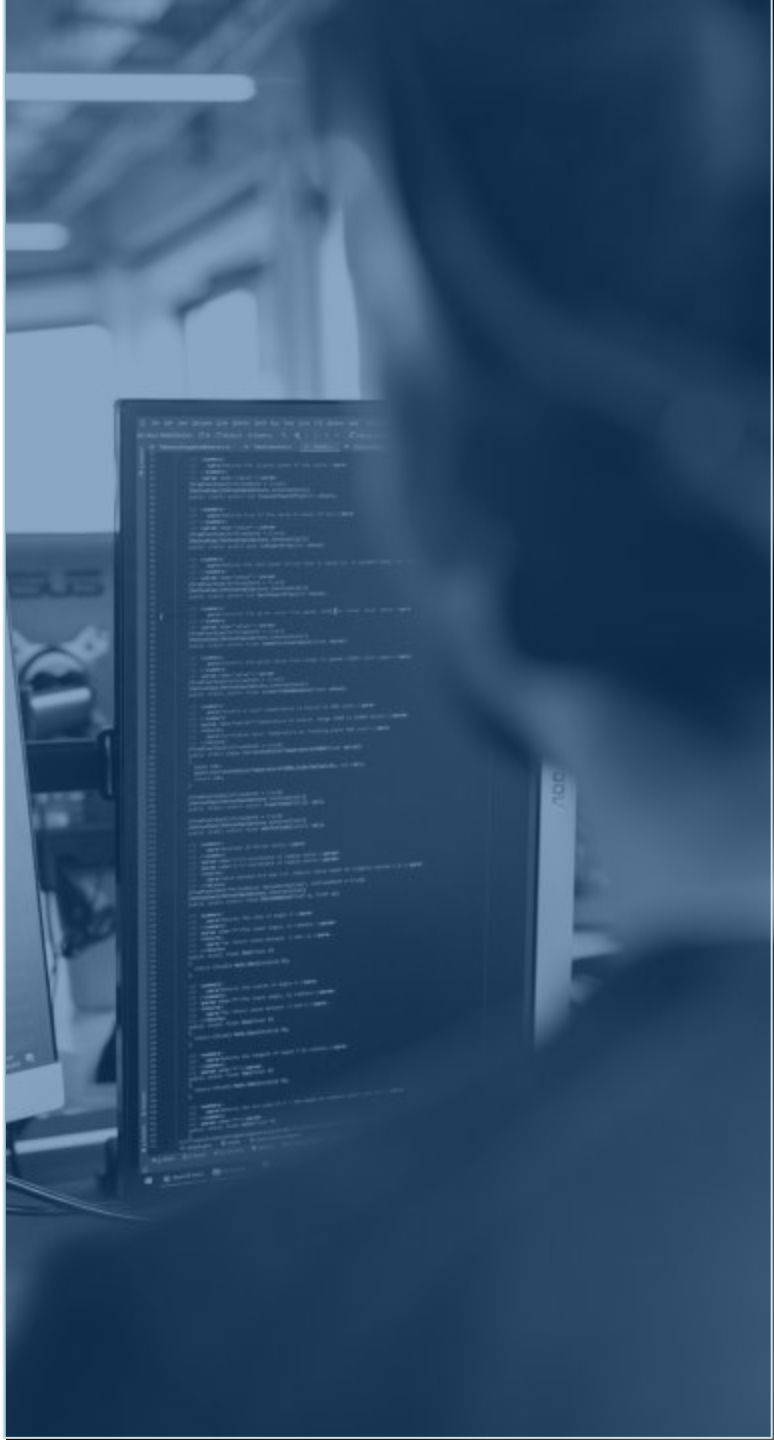
March, 2022

Powered by CYBERREADY

Por que é importante

A atividade cibernética que envolve o conflito entre a Rússia e a Ucrânia está a aumentar e, ainda que não estejamos diretamente envolvidos no conflito, todos somos afetados.

Todas as crises mundiais têm uma dimensão cibernética e o aumento acentuado dos e-mails de phishing maliciosos mostra que esta crise não é diferente.



O que se está a acontecer

1. Ambos os lados lançaram ciberataques um contra o outro que incluem malware de eliminação de dados e a desativação de sites para evitar a sua utilização legítima.

2. Nem sempre estes ataques são controlados e infetam frequentemente dispositivos e sites que não estão envolvidos no conflito. Isto inclui igualmente os seus dispositivos empresariais ou pessoais.

3. As suas contas nas redes sociais também estão em risco de serem alvo de acessos ilícitos e utilizadas como meio de distribuição de informações falsas ou malware.

O que pode fazer para proteger a sua rede doméstica

Se estes estiverem disponíveis, deve ver uma notificação no seu computador ou telemóvel. Se estes estiverem disponíveis, deve ver uma notificação no seu computador ou telemóvel.

Adicione um segundo fator de autenticação às suas contas nas redes sociais (Facebook, LinkedIn, Twitter, etc.) e às suas contas de e-mail. Se possível, adicione também um e-mail de cópia de segurança.

Informe os seus amigos e familiares do que se está a passar e incentive-os a fazer o mesmo.

O que pode fazer para proteger a nossa rede

Estamos a tratar da segurança da rede interna, pelo que não há nenhuma ação técnica que tenha de efetuar.

Durante estes períodos pode sofrer mais ataques de phishing. Tenha cuidado com os e-mails que solicitam a sua assistência em questões técnicas ou financeiras.

Verifique sempre o endereço do remetente - lembre-se de que este é o passo mais importante para detetar ações de phishing.