BOAS PRÁTICAS DE CIBERSEGURANÇA PARA CARGOS PÚBLICOS

Como promovo a cibersegurança da minha organização? *CHECKLIST*

QUANDO UTILIZO *EMAIL*

1. Só abro *emails* que conheço - verifico o endereço e não o nome;
2. Caso abra *email* suspeito, não clico em *link* ou anexo e reporto à Equipa de Segurança Informática;
3. Não envio por *email* Informação Classificada de Marca Nacional e Grau superior a Reservado;

QUANDO UTILIZO TELEMÓVEL, PORTÁTIL OU *PENS* USB

4. Para fins profissionais, apenas uso dispositivos autorizados;
5. Ativo o bloqueio automático e não deixo dispositivos desbloqueados;
6. Uso *passwords* ou PIN e limite de tentativas para acesso;
7. Cubro ou desativo a câmara de portátil - ativo apenas quando necessário;
8. Utilizo filtros de privacidade no ecrã do portátil;

QUANDO UTILIZO *PASSWORD*

9. Mantenho-a secreta – e não a guardo em listas ou *browsers*;
10. Uso *passwords* com mais de 10 caracteres, com maiúsculas, minúsculas, algarismos e caracteres especiais - não uso termos previsíveis (ex.: nome da cidade de origem);
11. Altero-a regularmente (ex.: de 2 em 2 meses);
12. Uso-a numa só plataforma (ex.: uma, no *email*; outra, numa rede social; etc.);

QUANDO VIAJO

13. Antes de viajar: atualizo as aplicações e *software*; limpo o histórico de chamadas, do *browser* e os *cookies*; não publico planos de viagem nas redes sociais;
14. Durante a viagem: vigio os dispositivos; se tiver de me separar deles, retiro o cartão SIM e, se possível, a bateria; não carrego a bateria dos equipamentos em terminais públicos ou dispositivos não controlados;
15. Depois da viagem: altero as *passwords* usadas na viagem; volto a limpar o histórico de chamadas, do *browser* e os *cookies*;

QUANDO ME LIGO À *INTERNET* E NAVEGO

16. Utilizo VPN da organização quando uso redes Wi-Fi públicas;
17. Só uso serviços de armazenamento em nuvem autorizados;
18. Mantenho sempre o *bluetooth* desligado;

QUANDO TROCO MENSAGENS

19. Tenho os mesmos cuidados no uso de sms do que no uso de *email*;
20. Não envio informação confidencial por WhatsApp ou serviços semelhantes.

Sabia que...?

- O *email* e o *phishing* são os principais modos através dos quais há infeções por *malware*.
- Milhões de *passwords* são expostas todos os anos.
- 85% dos *emails* mundiais são *spam*.
- O roubo de dispositivos é uma porta aberta para o furto de dados.
- O Setor Público é dos setores mais afetados pelo furto de dados.
- A Ciberespionagem é uma das principais ameaças e é cada vez mais usada pelos Estados.
- Estados patrocinam cibercriminosos tornando os ataques com motivos políticos mais sofisticados.
- O comportamento (hábitos de ciber-higiene) é fundamental para uma boa defesa contra ciberataques.
- Com a Internet das Coisas, qualquer dispositivo ligado à *internet* é um potencial alvo de ciberataques.

ENISA Threat Landscape Report 2018 (2019)

Em caso de dúvida, envie-nos um email ou telefone que nós esclarecemos.
Para aceder a mais documentação, consulte o nosso website: www.cncs.gov.pt

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

CNCS Centro Nacional de Cibersegurança PORTUGAL