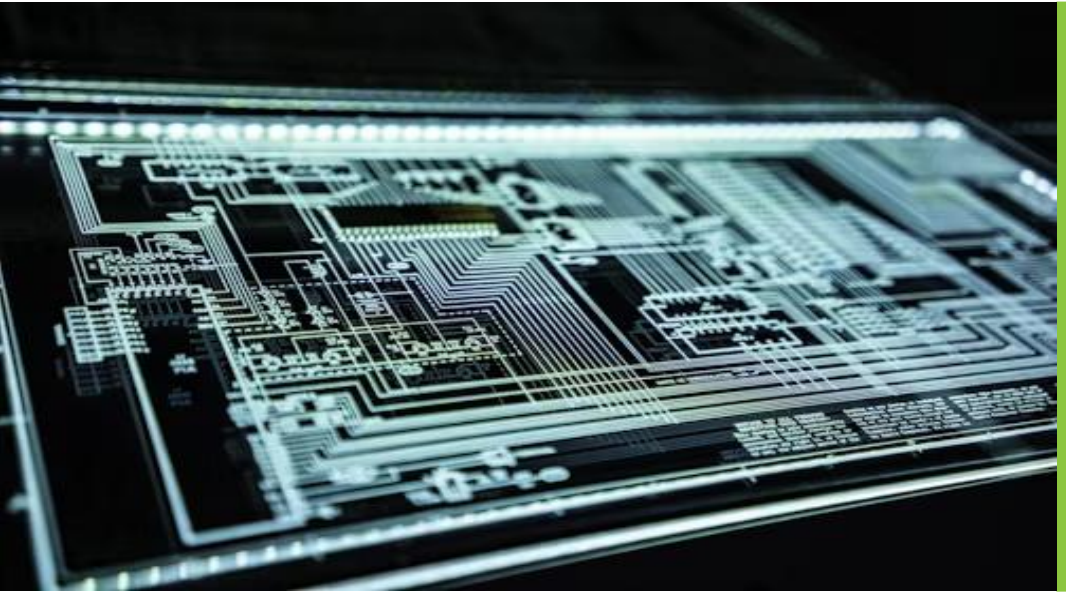

Cibersegurança

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Introdução

Vivemos cada vez mais ligados ao mundo digital, o que traz inúmeras vantagens, mas também novos riscos.

Proteger os nossos dados e equipamentos é fundamental para evitar fraudes, perdas de informação e outros problemas graves.

Neste guia, vais encontrar dicas simples e práticas para te protegeres online, seja em casa, no trabalho ou em qualquer lugar.

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Engenharia Social – O que é?

A engenharia social é uma técnica de manipulação psicológica usada para enganar pessoas e obter informações sensíveis.

Exemplos de ataque:

- Isco para despertar curiosidade ou medo
- Linguagem semelhante à do local de trabalho
- Sentido de urgência/emergência
- Pedidos de resposta rápida por SMS, e-mail ou telefone

Como Evitar Ataques de Engenharia Social

- Não responder a mensagens ou e-mails de contactos desconhecidos
- Desconfiar de ofertas e promessas
- Nunca clicar em links ou anexos de fontes duvidosas
- Ler sempre com calma, mesmo que a mensagem pareça urgente
- Nunca partilhar pins, passwords ou dados sensíveis por mensagem

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Perigos no Correio Eletrónico e Mensagens

- E-mails e mensagens podem imitar empresas reais
- Pedem para descarregar anexos ou clicar em links falsos
- Objetivo: roubar informações pessoais ou instalar malware

Como prevenir:

- Verificar sempre o remetente
- Não abrir anexos ou links suspeitos
- Confirmar a autenticidade antes de responder

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Navegação Segura na Internet

- Sites maliciosos podem instalar malware ou roubar dados
- Podem imitar páginas legítimas para enganar o utilizador

Boas práticas:

- Manter o sistema e software sempre atualizados
- Usar antivírus, mas não confiar só nele
- Fechar imediatamente sites suspeitos
- Nunca introduzir credenciais em páginas duvidosas

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Palavras-passe Seguras

- Usar passwords longas (mínimo 14 caracteres), com maiúsculas, minúsculas, números e símbolos
- Evitar informações pessoais
- Alterar periodicamente e não repetir passwords antigas
- Não usar a mesma password em vários serviços
- Sempre que possível, ativar autenticação de dois fatores
- Não guardar passwords no navegador

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Equipamentos e Redes Seguras

- Não ligar pens/discos USB desconhecidos ao computador
- Não usar dispositivos pessoais em computadores públicos
- Formatar dispositivos antes de os descartar ou entregar a terceiros
- Não deixar passwords anotadas em locais visíveis
- Bloquear o computador quando não o usas

Redes Wi-Fi Públicas – Riscos e Cuidados

- Evitar redes Wi-Fi públicas ou desconhecidas
- Preferir dados móveis ou VPN
- Confirmar sempre o nome da rede com o local
- Desligar Wi-Fi/Bluetooth quando não usados
- Nunca aceder a informações sensíveis em redes públicas
- Terminar sempre sessão nas contas
- Atenção a ataques como hotspots falsos, malware e man-in-the-middle

Projeto Nr. - 2023-1-TR01-KA220-ADU-0160651

Conclusão - Pequenas Ações, Grande Diferença

A cibersegurança depende de cada um de nós. Ao adotares boas práticas, consegues reduzir drasticamente o risco de seres vítima de ataques ou fraudes.

Mantém-te informado, atento e nunca subestimes a importância de proteger os teus dados e dispositivos.

Lembra-te: a tua segurança online começa com as tuas escolhas diárias!

Auto-avaliação