FORMAÇÃO DE CIBERSEGURANÇA COM OS GÉNIUS! CLARO.

Formação
Cyber Security
Awareness

SABER MAIS



TFD Formação de Desenvolvimento

TRIGÉNIUS TECNOLOGIA

Trigénius Tecnologia...

FORMAÇÃO CYBER SECURITY AWARENESS

FORTALEÇA O LADO HUMANO DA SUA SEGURANÇA E REDUZA O RISCO CIBERNÉTICO

Proporcione níveis mais elevados de envolvimento através de formação personalizada e focada em consciencialização sobre cibersegurança.



AUMENTE RAPIDAMENTE O CONHECIMENTO

De forma simples tomar consciência do que temos de mudar no nosso dia a dia.



INFLUENCIE COMPORTAMENTOS A LONGO PRAZO

Com dados abrangentes, métricas e insights baseados na ciência comportamental.



CONTINUE A PROMOVER A SEGURANÇA

Os hábitos diários de Ciberhigiene são essenciais para a segurança.

O QUE VAI APRENDER



Conhecimentos e as Atitudes Essenciais para a adoção de comportamentos responsáveis no Ciberespaço



Identificar e Compreender as Principais Ameaças aos ambientes digitais das empresas e das pessoas



Proteger os Dados Pessoais e a Privacidade em ambientes digitais, dispositivos e conteúdos digitais



Identificar Formas de Proteção e Medidas de Segurança tendo em conta a confiabilidade e a privacidade na utilização dos dispositivos digitais das empresas e pessoais

A QUEM SE DESTINA

- Colaboradores em Ambiente Empresarial;
- Publico Geral;

EM CONFORMIDADE COM AS NORMAS

Cumprimos com os requisitos globais de conformidade de segurança da informação:

- National Institute of Standards and Technology (NIST) 800-115;
- ISO 27001;
- Quadro Nacional de Referência para a Cibersegurança (QNRCS).

TRIGÉNIUS TECNOLOGIA

FORMAÇÃO CYBER SECURITY AWARENESS

OS CIBERATAQUES EM PORTUGAL AUMENTARAM MAIS DE 716% DE 2015 A 2023

Os criminosos estão cada vez mais sofisticados a explorar falhas como passwords fracas, softwares desatualizados, ou definições de segurança mal configuradas.

PRINCIPAIS TIPO DE INCIDENTES EM PORTUGAL

Phishing/Smishing	35%
Tentativa de login	19%
Engenharia Social	10%
Comprometimento de conta não privilegiada	7%
Distribuição de Malware	6%

Registados pelo CERT.PT em 2023

CENÁRIO GLOBAL

59% **De todas as organizações** foram atingidas por ataques de ransomware no último ano.

70% **Das violações de dados** causaram interrupções significativas ou muito significativas.

41% **Das pequenas empresas** sofreram uma ameaça cibernética.



A PREVENÇÃO É A MELHOR DEFESA

ALERTA + **SABER** = **CUIDADO**

- O Ciberespaço apresenta muitas ameaças;
- A Cibersegurança procura proteger-nos dessas ameaças;
- O Cibercrime tem muitos custos para as organizações;
- Os Ciberatacantes reconhecem e depois exploram o alvo;
- Os ataques mais comuns aproveitam-se da informação que disponibilizamos ou de ligações maliciosas a que acedemos.

TRIGÉNIUS TECNOLOGIA

FORMAÇÃO CYBER SECURITY AWARENESS

CIBER(IN)SEGURANÇA
SERÁ QUE SOU "CIBERINGÉNUO"?

Os atacantes recolhem informação sobre o alvo e usam isso para tornar a mensagem mais credível e o ataque mais preciso.

KILL CHAIN

Etapas de um ataque, para compreender, detectar e interromper em vários estágios.

PREPARAÇÃO DE UM ATAQUE
DE 1 A 3

1. **RECONHECIMENTO**
2. **ARMAMENTO**
3. **DISTRIBUIÇÃO**
4. **EXPLORAÇÃO**
5. **INSTALAÇÃO**
6. **COMANDO & CONTROLO**
7. **AÇÃO**

ATAQUE INFORMÁTICO
DE 4 A 7

PHISHING

Uso de engenharia social para que os destinatários **"mordam um isco"**.



Desconfiaria deste tipo de mensagem ou email?

Estimado cliente,

Pedimos-lhe que reveja os seus dados pessoais.

Verifique a sua identidade com os dados facultados.

https://seguro-portal.info

Identificaria estes websites maliciosos?

- www.glthub.com — Typos
- www.gougle.com — Typos
- www.amozon,com — Typos
- www.victoriasecret.com — Falta o "s"
- www.homdepot.com — Troca de letras

TRIGÉNIUS TECNOLOGIA

FORMAÇÃO CYBER SECURITY AWARENESS

A PROTEÇÃO É RESPONSABILIDADE DE TODOS

Hoje, mais que nunca, vivemos em rede!
Uma rede com tecnologia... E com pessoas!

O MATERIAL TEM SEMPRE RAZÃO

A responsabilidade pela Cibersegurança é sempre das pessoas!
Não da tecnologia.

Um simples gesto pode abrir a porta ao cibercrime:

- Abrindo um anexo malicioso;
- Clicando num URL inseguro;
- Introduzindo passwords em páginas de aparência legítima.

Perigos do Cibercrime

- **FURTO DE IDENTIDADE**
- **ACESSO E BLOQUEIO DE ARQUIVOS E DISPOSITIVOS**
- **EXFILTRAÇÃO DE DADOS SENSÍVEIS E PRIVADOS**
- **SOFRER DE CHANTAGEM E RESGATE MONETÁRIO**



TODOS SOMOS AGENTES DE SEGURANÇA

Todos somos responsáveis pela nossa segurança

Falamos?
Solicite contacto ou agende uma demonstração.

TRIGÉNIUS TECNOLOGIA

FORMAÇÃO CYBER SECURITY AWARENESS

CIBERHIGIENE
PRECISAMOS DE ADOTAR UM MANUAL DE BOAS PRÁTICAS

O comportamento humano é a peça chave da Cibersegurança e um manual de boas páticas, ainda que simples, é uma mais-valia importante para qualquer empresa;

EMAIL	PASSWORD	REDES SOCIAIS	HARDWARE	NAVEGAÇÃO WEB
DESCONFIAR	**COMPLICAR**	**PRESERVAR**	**BLOQUEAR**	**PREVENIR**

DESCONFIAR EMAIL

- Abrir apenas emails de origens conhecidas;
- Caso abra um email, não clicar em nenhum anexo ou link;
- Verificar o endereço do remetente e a veracidade do email;
- Não enviar informação sensível por email.

COMPLICAR PASSWORD

- A password é essencial para proteger informação pessoal e empresarial;
- O comprometimento da password pode resultar em roubo de identidade e data breach;
- Deve sempre alterar uma password pré-definida.

PRESERVAR REDES SOCIAIS

Há que ter consciência que:

- Adica dos direitos de uma imagem que publique nas redes sociais;
- Quando usa a autenticação das redes sociais está a partilhar dados seus;
- Aquilo que publica pode ser utilizado "**Uma vez na net, sempre na net!**".

TRIGÉNIUS TECNOLOGIA

FORMAÇÃO CYBER SECURITY AWARENESS

OS HÁBITOS DIÁRIOS DE CIBERHIGIENE SÃO ESSENCIAIS PARA A SEGURANÇA

Adotar o comportamentos e práticas certas em cada um dos pontos referidos, é o meio caminho para Ciberseguro e Ciberresponsável.

BLOQUEAR HARDWARE

- Tapar ou desligar câmaras e microfone quando estes não forem necessários;
- Bloquear equipamentos, não abandonar dispositivos desbloqueados;
- Não utilizar pendrives USB de origem desconhecida;
- Evitar olhares de terceiros, sejam pessoas próximas ou câmaras de vigilância;
- Proteja/bloqueie as portas USB dos seus equipamentos.

PREVENIR NAVEGAÇÃO WEB

Prevenir é estar atento a como navegamos:

- Evite ligar-se a Wi-Fi público, pode permitir o acesso aos seus dados;
- Desconfie de aplicações duvidosas;
- Em sites bancários verifique o certificado digital do site;
- Nas compras online, devemos validar informação do vendedor;
- No teletrabalho, redobre os cuidados com a ligação e os dispositivos.



TRIGÉNIUS TECNOLOGIA

ENTÃO, ESTÁ DECIDIDO? FALE CONNOSCO. AVANCE.

Somos todos ouvidos.

CLIQUE AQUI

trigenius.pt

Escolha online o que prefere:
Agendar Reunião | Solicitar Visita
Chamada Telefónica | Contacto por e-mail

TRIGÉNIUS
TECNOLOGIA

contacto@trigenius.pt
+351 249 530 800
Fátima, Lisboa

v.01-10.2025