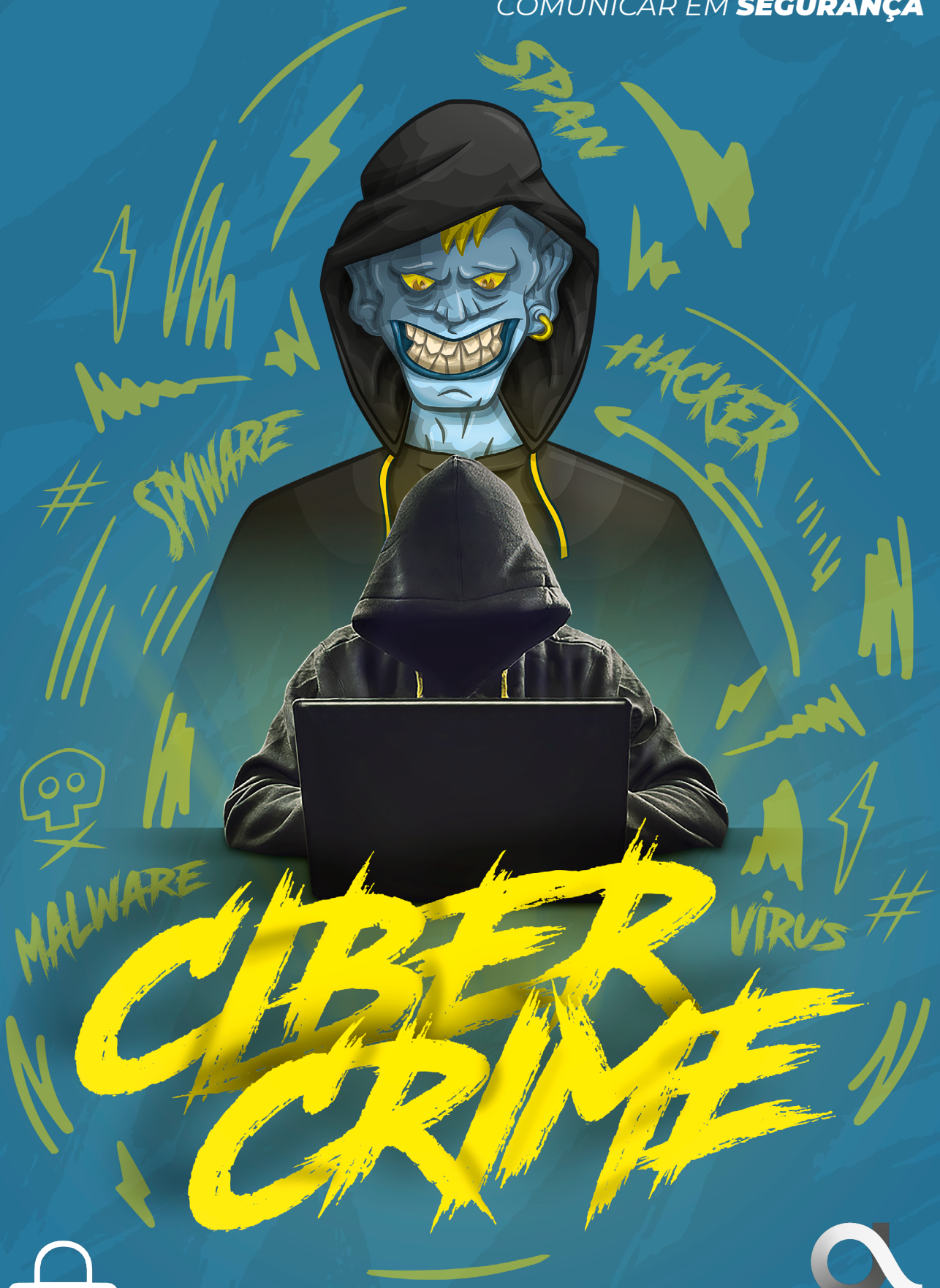
COMUNICAR EM **SEGURANÇA**



COMUNICAR EM SEGURANÇA

altice fundação

RANSOMWARE

PHISHING

BURLAS ONLINE

CRIAÇÃO DE PERFIL FALSO

ROUBO DE DADOS PESSOAIS

CYBERBULLYING

AFINAL NÃO ACONTECE SÓ AOS OUTROS....

E AGORA, O QUE FAÇO?

O QUE É?

Cibercrime é o nome dado a qualquer prática ilícita e ilegal praticada através de meios informáticos. São crimes direcionados a equipamentos tecnológicos (computadores, tablets, telemóveis, etc) e redes, realizados através da Internet. Caso não existisse Internet, estes crimes não existiriam.

O cibercrime engloba várias práticas como o roubo de dados pessoais, instalação de vírus e malware , criação de perfis falsos na Internet(por exemplo nas Redes sociais ou para praticar esquemas de fraude) , burlas online ou cyberbullying.

Uma das grandes dificuldades no combate ao cibercrime é a sua característica transnacional. Em muitas situações, existe uma grande dificuldade em identificar a origem do crime e os seus autores. Uma pessoa pode ser vítima de um cibercrime feito noutro país que não o seu, o que levanta muitas dificuldades no combate a este tipo de crime e consequente punição. Cada país tem o seu enquadramento legal para o cibercrime, e é frequente não existir qualquer punição ou leis para o cibercrime.

Utilizando cada vez mais Internet e equipamentos tecnológicos, é fundamental que os utilizadores tenham conhecimentos na área da Tecnologia, Redes e Cibersegurança de forma a conseguirem proteger-se e evitar este tipo de situações.

Muitas situações de burla online, esquemas de fraude, roubo de dados pessoais podem ser evitados com comportamentos mais conscientes e preventivos. Muitos cibercriminosos “aproveitam-se” do desconhecimento e imprudência dos utilizadores para praticarem os crimes. No entanto, as vítimas deste tipo de crime tanto podem ser pessoas singulares, como empresas.

TIPOS DE CYBER CRIME

RANSOMWARE

É um tipo de malware (programa malicioso) que provoca o bloqueio do sistema operativo e equipamentos até que o resgaste seja pago. O resgaste é sempre virtual, e normalmente, acontece através do uso de uma moeda virtual, designada por bitcoin. Este crime é praticado através do envio de emails de phishing ou sites falsos, recorrendo à Engenharia Social.

ROUBO DE DADOS PESSOAIS

Furto de informações pessoais confidenciais como dados de cartão de crédito, dados bancários, conta de email, para depois estas informações serem vendidas ou para atos ilícitos. Este crime acontece muitas vezes recorrendo à Engenharia Social ou envio de e-mails direcionados para conseguirem obter os dados das pessoas.

STALKING E REVENGE PORN

Os relacionamentos online podem conduzir a situações de cibercrime. Neste tipo de relações, as pessoas partilham os seus dados pessoais como fotografias, vídeos, emails, passwords e posteriormente podem ser vítimas deste tipo de crime.

A partilha de fotografias e vídeos íntimos(sexting) pode levar a casos de revenge porn e sextortion, ou seja, à partilha não autorizada de fotografias e vídeos íntimos e ameaças. É uma situação muito frequente no final de relações pessoais. Também é considerado crime o Stalking, ou seja, a perseguição online de pessoas através de meios tecnológicos. Os agressores podem ser conhecidos ou desconhecidos da vítima, sendo um crime extremamente intrusivo.

BURLAS ONLINE

As burlas online podem ser de cariz financeiro ou pessoal/amoroso. Existem as burlas de comercio eletrónico mais simples como uma compra online cujo material nunca se recebe embora tenha sido feito o pagamento ou sites que conseguem armazenar dados bancários dos utilizadores. As burlas bancárias têm muitas vezes origem no envio de emails de phishing. Os utilizadores acreditam que estão a aceder ao seu banco, e dão os seus acessos (login e password) aos criminosos.

As burlas nos relacionamentos amorosos (romance scams) estabelecem-se quando o criminoso consegue estabelecer uma relação pessoal e de confiança com a vítima para, de seguida, cometer extorsão financeira e burla.

CYBERBULLYING

O cyberbullying pode ser visto como uma forma ou extensão do bullying que é realizado através de meios digitais, sendo também um comportamento agressivo, intencional e continuado. Pode acontecer em qualquer local, a qualquer hora, constantemente.

O agressor é, muitas vezes, anónimo, existe um distanciamento físico, as agressões chegam através dos telemóveis, redes sociais e mensagens , contribuindo desta forma para a complexidade do fenómeno e para o agravamento das consequências emocionais das vitimas.

DICAS E SUGESTÕES

Ter atenção a e-mails suspeitos:
Verificar a origem/remetente do e-mail;
Verificar se existem erros ortográficos;
Ter atenção a links ou anexos.

Compras Online:
Pesquisar se é um site credível e seguro (ex: https, cadeado); Usar um sistema de pagamento seguro (ex:Paypal, Multibanco,MBnet, contrareembolso).

Anti-Vírus e Firewall
instalado e atualizado.

Ter passwords fortes
e diferentes para cada site.

Fazer backups regulares
para evitar perder informação.

Utilizar redes Wifi seguras ou VPN.

Manter o software atualizado.

Manter os dados e informações pessoais privados ou bloqueados nas Redes Sociais.
A Engenharia Social recorre a este tipo de dados.

Não aceitar contactos de pessoas estranhas.

Não partilhar fotografias/vídeos com desconhecidos.

Não enviar fotografias ou vídeos íntimos
que possam ser usados para sextortion/revenge porn.

Em situações de Cyberbullying, pedir ajuda é essencial.

Guardar comprovativos de email e mensagens
para serem material de prova.