Canais oficiais para denúncia:

- Youtube: para denunciar um vídeo impróprio ou que atente contra o direito de alguém, basta acessar https://www.youtube.com/yt/policyandsafety/pt-BR/reporting.html e preencher o formulário específico disponível.
- Twitter: acessar o link https://support.twitter.com/forms/abusiveuser e preencher o formulário disponível.
- Facebook: para denunciar conteúdo abusivo ou spam deve-se usar o botão "Denunciar", que aparece ao lado do próprio conteúdo, e acessar https://www.facebook.com/help/181495968648557/.
- WhatsApp: quando se recebe uma mensagem inicial de um contato desconhecido, há a opção "Denunciar" como spam e bloquear. Isto fará com que esse usuário seja reportado e o mesmo será adicionado à lista de contatos bloqueados.
- Instagram: para denunciar o conteúdo diretamente pelo aplicativo basta clicar no botão ou funcionalidade que aparece junto com o mesmo. Se não possuir uma conta, deve-se acessar https://help.instagram.com/contact/383679321740945.

Centro Universitário
UniProcessus - Campus Águas Claras

Av. das Araucárias, 4400 - Águas Claras, Brasília - DF, 71936-250
Telefone: (61) 3562-6343

UNI PROCESSUS centro universitário

UNI PROCESSUS centro universitário

Crimes Cibernéticos

DIREITO DIGITAL

Marcus Eduardo
Bernard Benson
Glênia de Sousa
Ires Pimenta
João Carlos
Júlio César
Letícia Lima
Maria Eduarda
Matheus Viana
Nícolas Souza

O que são crimes cibernéticos?

São aqueles crimes que utilizam computadores, redes de computadores ou dispositivos eletrônicos conectados para praticar ações criminosas que geram danos a indivíduos ou patrimônios, seja por meio de extorsão de recursos financeiros, estresse emocional ou danos à reputação de vítimas expostas na Internet.

Por ser um tipo de crime dependente da ação ou inação humana, a melhor forma de prevenção é justamente por meio da conscientização da população, especialmente das classes mais baixas.

Recomendações

I) não abrir arquivos anexados, pois geralmente são programas executáveis que podem causar danos ao computador ou capturar informações confidenciais;

2) não clicar em links para endereços da Internet, mesmo que conste o nome da empresa ou instituição, ou, ainda, mensagens como “clique aqui”;

3) em caso de dúvidas sobre a origem e veracidade de determinada mensagem, procurar excluir o e-mail evitando executar seus anexos ou acessar os links presentes em seu conteúdo;

4) em casos de contaminação por vírus ou outro código malicioso, reformatar a máquina, reinstalar totalmente o sistema operacional e os aplicativos, evitando restaurar backups antigos;

5)não emprestar sua senha de e-mail, de Internet, de rede da empresa, de cartão de crédito, de conta bancária em hipótese alguma;

6) evitar baixar aplicativos gratuitos só porque são de graça, buscar referências e recomendações de quem já os utiliza, visto que muitos golpistas têm utilizado aplicativos falsos para contaminar o equipamento do usuário e capturar dados do mesmo;

7) utilizar softwares de proteção (antivírus, antispam, antispyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas;

8) duvidar do perfil de pessoas que se comunicam em ambientes não seguros e anônimos, como mídias sociais, evitando clicar e abrir imagens, e fazendo a verificação ou confirmação de identidade sempre que possível (se a pessoa é quem diz ser); e

9) registrar a ocorrência na delegacia mais próxima ou na especializada em crimes eletrônicos.

Escaneie o QR-Code para ter acesso a cartilha do TJDFT sobre segurança virtual: