Cybercrime in the UAE: Laws, Penalties, and How to Stay Safe Online

Introduction:

DR.
HASSAN
ELHAIS

Cybercrime is a major social threat to individuals and organizations in the UAE. The government of the UAE has already implemented a structured legal system to prevent such online crimes. According to **UAE criminal law**, these offenses are taken very seriously with strict penalties. By understanding the cybercrime laws and staying vigilant against online crimes, individuals can protect themselves from becoming victims. Prompt reporting may prevent or reduce cybercrime incidents and contribute to a safer cyberspace.

What are the major online crimes and their punishments under the UAE's cybercrime laws?

The major **cybercrimes in the UAE** include hacking, damaging government agencies' computer networks, infringing on private data, fabricating emails, websites, and digital accounts, as well as illegally monitoring and disseminating data. Under **criminal law in UAE**, depending on the offense's severity and the case's circumstances, a conviction can lead to a fine, jail time, or both. Article 11 of the cybercrime law prohibits creating fraudulent websites or email addresses or misrepresenting others with imprisonment and AED 50,000–200,000 fines. Further, using fake accounts to damage someone may get the offender jailed for two years. Targeting state institutions' websites or accounts carries penalties that escalate to AED 200,000 to AED 2,000,000 in fines and five years in prison.

What are the most common tactics used to commit the online crimes in the UAE?

Sending fake web links through messages or emails is known as smishing. It may direct the users to scam websites that illegally collect information, such as financial information and personal data. These kinds of scams can result in substantial financial losses and the misuse of the users' identities.

The criminal activity that can occur online is known as hacking. This procedure is a frequent practice in which individuals and even businesses receive requests for sensitive information such as banking and credit card information through emails that appear legitimate. Being a victim of phishing scams can result in financial fraud and risking private data.

Another very common way of online scamming is through phone calls, called voice phishing. Scammers may use phone calls to trick victims into sharing sensitive information or transferring money. The banks and government authorities may initiate campaigns to raise awareness and prevent such online fraud activities. It's important to note that legitimate organizations will never request sensitive information over the phone.

How to protect yourself from cyberattacks?

Beware and avoid sharing personal data and contact information on untrusted internet sites. It is extremely important to remain vigilant when downloading from unknown links that are received via text messages or emails. Download apps only from authorized sources, ensure your personal data is kept safe, and create backup copies. Regularly monitor for signs of electronic fraud, such as abnormal battery consumption or slower processing speeds.

Conclusion:

Cybercrime victims may report the incidents to the nearest police station. In each emirate, official websites and applications are created by relevant authorities to submit cybercrime complaints. The federal public prosecution established an application named My Safe Society to report suspicious activities on social networking websites that may impact national security or public order.