GOA POLICE

Pharming is a scam where a fraudster installs malicious code on a personal computer or server. This code then redirects any clicks you make on a website to another fraudulent Website without your consent or knowledge.

Cyberstalking means virtually following a victim online anonymously. Most of the victims of cyberstalking are women and children.

Social Media Imposter Profile:- Creating a profile on social media using the name or photograph or both of another person to create a impression that the profile belongs to a particular person. Sometimes the mobile number of particular person is also given.

Fraudvertisingis like malvartising but here the website will have advertisement with various offers. Once clicked on these adds, they will be redirected to fake website with variousoffers or business opportunities which is actually fraud.

Malvertising is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click on these ads they will be redirected to fake websites or a file carrying viruses and malware which will be automatically downloaded.

GOA POLICE

Cyber Crime prevention tips

Awareness is the master tip to prevent Cyber Crimes

- ✓ Beware of the latest Cybercrimes and its nature.
- ✓ Beware of Phishing emails, vishing calls and smishing messages.
- ✓ Never share your bank credentials, such as Account No. DEBIT OR CREDIT Card No, OTP with anyone over email phone call or SMS.
- ✓ Never make friendship with strangers on the internet, and do not fall prey to their story, sympathy and or gift offers.
- ✓ Do not blindly believe in adds that pop on the internet.
- ✓ Share minimum personnel information over the internet.
- ✓ Avoid giving your credit card or ATM cum debit card to strangers at the ATM for cash withdrawal.
- ✓ Use strong password and change them periodically.
- ✓ change all default passwords.
- ✓ Never allow strangers to use your phone or computer.
- ✓ Skip emails and messages that you do not recognize.
- ✓ Double check that the site you are visiting for purchase is a genuine site.
- ✓ Always use a genuine software and regularly update them.

- ✓ Do not store your password or bank details in plain readable text on the phone.
- ✓ Avoid downloading from the internet. Do not download just because it's free.
- ✓ Stay connected to the internet only when required.
- ✓ Double check that the customer care number you are calling is a genuine number, especially when the number is obtained from search engine such as Google Bing etc.
- ✓ Always have the practices of typing the website address rather than clicking on the search results.
- ✓ While doing online transactions make sure that the website address is starting with Https:// ("S" is very important).
- ✓ Be wise when you see unrealistic offers on the intent.
- ✓ If you feel you are a victim of bank fraud, immediately inform your bank and block your account.
- ✓ Report the fraud to the concern bank at the earliest.
- ✓ **If you feel you are a victim of Cyber Crime, contact the Cyber Crime Police station or Goa Police immediately.**

GOA POLICE

Cyber Crime Police Station,
Ribandar, Tiswadi, Goa
Pin:- 403006
Phone:- 0832-2443201
Mobile:- 7875756171
Email:- picyber@goapolice.gov.in
www.goapolice.gov.in/web/guest/cyber-crime-police-station
www.cybercrime.gov.in

@CyberDost

GOA POLICE

Cyber Crime Awareness

Cybercrime is a unlawful act where the computer is used either as a tool or a target or both. Cybercrime can be also defined as any criminal activity that takes place in the cyberspace.
Hacking, Phishing, Vishing, Smishing, Cyber defamation, identity theft, online fraud, Ransomware, Social Engineering, sexting, pornography, Malvertising, Fraudvertising, Cyberstalking, are some of the common Cyber Crimes.

Cyber Crime trends in Goa

Phishing means sending emails which resembles that of a genuine party, but not genuine, and the victim is tricked to share confidential information or data.

Vishing is a social engineering technique through phone calls to trick you into providing information or data.
Smishinguses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number.

Cyber Defamation
Cyber Libel: Defamation which is written such as on a web site.
Most online defamation occurs through libel by posting a web page, comment, bulletin board post, review, rating or blog post

Slander: Defamation that is spoken such as through an transcribed audio file.

Online Fraud
(Social Media Fraud) is a type of fraud where one ischeated through a fake profile created on popular social media platform.
Here the fraudster first studies the victim profile and then creates a profile of a wealthy individual or depending on the interest of victim, on popular social media platform.Then sends a friend request.Once friend request is accepted, the fraudster frequently keep communicating with the victim and gain more information of the victim and also his/her trust and confidence. Then using social engineering and cooking up a story of sending gift or business offer lure the victim to deposit money into various bank accounts. The victim in the belief of getting gift or business deal or out of sympathy keeps on depositing money upto a point where the victim is not in a positon to pay more.