HOW TO RECOGNIZE & PREVENT CYBERCRIME

Cybercrime comes in many forms including identity theft, financial fraud, stalking, online bullying, hacking, and more. At best, cybercrime can cause major inconvenience and annoyance for a victim. At worst, cybercrime can result in financial ruin or even threaten a victim's reputation or personal safety.

How to recognize cybercrime:

CGRC's Cyber Security Awareness Campaign encourages all communities to recognize these three (03) common cybercrimes and to follow simple steps to protect yourself listed below;

1. Identity theft is the illegal use of someone else's personal information in order to obtain money or credit. How will you know if you've been a victim of identity theft? You might get bills for products or services you did not purchase. Your bank account might have withdrawals you didn't expect or unauthorized charges.
2. Phishing attacks use email to collect personal and financial information or infect your machine with malware and viruses. Cybercriminals use legitimate-looking emails that encourage people to click on a link or open an attachment. The email they send can look like it is from an authentic financial institution, e-commerce site, government agency, or any other service or business.
3. Imposter scams happen when you receive an email or call seemingly from a government official, family member, or friend requesting that you wire them money to pay taxes or fees, or to help someone you care about. Cybercriminals use legitimate- looking emails that encourage people to send them money or personal information.

How to prevent cybercrime:

Follow these simple tips from the CGRC's Cyber Security Awareness Campaign to help foster a culture of cybersecurity in your organization.

1. Keep a clean machine. *Update the security software and operating system on your computer and mobile devices. Keeping the software on your devices up to date will prevent attackers from taking advantage of known vulnerabilities.*
2. When in doubt, throw it out. *Stop and think before you open attachments or click links in emails. Links in email, instant message, and online posts are often the way cybercriminals compromise your computer. If it looks suspicious, it's best to delete it.*
3. Use stronger authentication. *Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account.*

CGRC takes cybersecurity seriously every day of the year. As part of this, we would like to provide you with tips and resources to protect yourself and your company. Our campaign is aimed at empowering the Pakistan public to be safer and more secure online. The main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community.