WHAT IS CYBERCRIME?

Cybercrime is a fast-growing area of crime with a very wide scope. It encompasses any criminal act that involves the use of a computer and a network, including crimes committed over the Internet. For example, online scams are considered to be cybercrimes but so is telemarketing fraud.

In Brunei, the general trend of cybercrime is on the rise, with many crimes reported in the media involving the use of social media, and are mostly related to financial crime.

First Cybercrime Conviction

The first cybercrime conviction in Brunei was for the unauthorised access into a wireless Internet connection and the use of a stolen credit card number to make BND2,720 worth of online purchases.

The suspect used the stolen identity and managed to get a series of online purchases approved from a website owner. The suspect was eventually caught and sentenced to six months' imprisonment for his first offence and received a further 22.5 months' jail term for his illegal credit card shopping spree, which was served out concurrently.

Why We Need To Know About Cybercrime

While the use of technology is certainly convenient and has improved the way we share information and conduct our daily lives, we cannot deny that each time we use the Internet for communication and financial transactions, we are exposed to a certain degree of vulnerability.

The reality is that all individuals and organization with a computer or a phone, which is simply connected to a network or the Internet, are at risk. If we do not take precautions, our connections could potentially be accessed and misused by cyber-criminals from anywhere in the world.

Things To Watch Out For

1. **Spam emails and SMS**

   Spam is usually electronic junk mail or generally unsolicited bulk email typically promoting attractive offers sent to a large number of users for the purposes of advertising, phishing and spreading malware.

   There is a significant increase in the amount of spam sent via email nowadays as barrier to entry and operating costs are low. Most email security measures do not view spam emails as a threat and usually do not prevent them from depositing in the inbox.

2. **Scams**

   Scams come in many different forms. The most common scam typically involves receiving a call from someone informing you that you have just won a big prize in a lottery. The caller will often try to get your attention first by saying "You don't have to worry about retirement now" or "You can now get a bigger house for the family." However, to access the prize money, you would have to pay some sort of 'processing fee'. Several transactions (often via

remittance) would have gone through before the victims finally realize that they have been scammed.

Some scammers resort to romance to bait their victims. They set up fake profiles on social media sites and pose under the disguise of attractive people. They would first gain your trust by initiating a relationship with you. Some will ask for financial assistance from you and disappear once they have your money. Some other elaborate schemes would have the scammer pose as a single man (often with lots of money) who has fallen in love with the victim (often middle-aged, single women). They would claim that they have sent a 'gift' which then becomes detained at some transit point on the way to the victim. "Customs officials" will soon get in contact and demand that the victim pays a 'processing fee' to release the gift.

3. Hacking

Hackers access personal information over the internet through various social networking platforms and e-mails. Sensitive information can be accessed, such as your location, information on your vacation, your children's information and in extreme cases your financial information. In some cases, hackers will create fake accounts on social networking sites to impersonate you in order to defraud your close friends and families.

Ways to Protect against Cybercrime

a. Use anti-virus software

Virus and other malicious software can easily be embedded inside innocent looking email attachments, downloadable files or websites. Be responsible and aware of what you are downloading, browsing and clicking on. Having anti-malware or anti-virus software installed will reduce the chances of your computer becoming infected by alerting you to potential threats.

b. Ignore pop-ups

Pop-ups can contain malicious software which can trick a user into verifying something. Once you perform downloads, there is a back-end install of malware. This is known as a drive-by download.

c. Two-factor authentication

If your email or social media services offer two-factor authentication, take the trouble to set this up. This means, in addition to entering your password, you are also asked to enter a verification code sent via SMS to your phone. So a hacker might crack your password, but without the unique and temporary verification code, they should not be able to access your account.

d. When shopping online, use secure websites

Before entering your card details, always ensure that the '*locked padlock'* or '*unbroken key'* symbol is showing on your browser's address bar. Additionally, the beginning of the online retailer's internet address will change from "http" to "https" to indicate a connection is secure. Be wary of sites that change back to http once you have logged on.

e. Other ways to avoid being victims of cybercrime are the following:

- Install encryption software
- Read up and improve your awareness of scams so you can avoid them
- Monitor your child's computer activities
- Be wary of strangers (of any gender) who ask to video chat with you as this may be recorded and used against you as blackmail
- Use secure passwords that cannot be easily guessed (do not use '12345'or 'password'), and change them frequently
- Keep your software up-to-date
- Do not use pirated software as these may contain viruses

Be Aware – do some investigation on your own to find out more. Download the "AMBD" app on your smartphone to learn more about the nature of financial scams.
Be Alert - there is no such thing as easy money.
Be Advised – contact your local authorities if you are suspicious.

How to report if you are a victim

Victims or individuals who suspects that they may have been targeted in a fraudulent attempt can:

1. **Report to the Police**

   File a report to the nearest police station on the incident and ensure you provide the police with as much information as possible.

2. **Contact your Bank**

   If you feel your account or other financial facilities have been compromised, do not hesitate to contact your bank to alert them about this.