CYBERCRIME

"is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them"

4 Things you can do to keep yourself safe from cybercrime

1. **Activate your multifactor authentication**
By implementing multifactor authentication on your accounts makes it less vulnerable from any cyber-attack.

2. **Update you software**
By Updating you software periodically is significantly reduce you risk to any cyber-attack.

3. **Think twice before you click**
Think again before you click any link because most cases of cyber-crime are coming from email phishing.

4. **Put on strong password**
Do not use the same password repetitively across all you apps and accounts.

Education about the dangers of cyber threats also needs to continue to be echoed through any media so that people are more digitally literate

"Tips for Cybercrime Protection & Combating Fraud"

Type of Cyber Crimes

DDos Attacks

Make an online service unavailable and take the network down by overwhelming the site with various traffic

Identity Theft

Gains access to a user's personal information

Social Engineering

Making direct contact with you by phone or email

Phishing

Hackers sending malicious email attachment or URLs to user

Online Scams

In the form of ads or spam emails that include promises or reward and offers

Cyberstalking

Cyberstalkers use social media, websites and search engines to intimidate user

PUPs

Potentially Unwanted Programs are less threatening that others, but a type of malware.

Exploit Kits

Bug in the code of a software in order to gain control of a user's computer

CYBERCRIME Cases

Email Sample targeted Attack Mail

Subject: Invitation to Information Security Seminar for F inancial I nstitutions

From :****@***.com

To: .....@abc.com

Dear Mr / Ms. **

In May 2020, a seminar will be held to report/ discuss results of corporate
survey jointly conducted by ○○ University and Zenginkyo
The briefing session, which is based on the results of the questionnaire, will
be of great help to financial institutions stakeholders in considering the future
direction of information security in financial institutions. Please also see the
reports attached.

We look forward to your active participation.
For details, see the invitation attached.
You can register for the seminar from the address below.
As seminar room capacity is limited, we recommend you to register as soon
as possible.

Register from⇒ https://www.abc.com

Attachments:

Subject and text are designed to attract targets.

It is necessary to confirm the source address carefully.
In recent years, it sometimes **pretends to be a real company or company email**

It is camouflaged to disguise part of the official website URL so that it cannot be distinguished from the real thing at a glance.

Also, the link destination may be written in meaningful words so you may need to check the actual link destination.

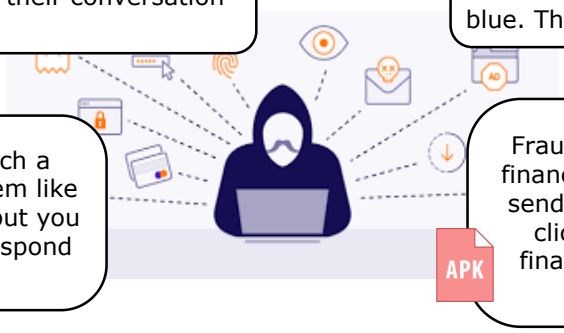
For Word/Excel and CSV files etc.
Targeted attack emails using Microsoft Office are
on the rise. File extensions can be impersonated.

Attaching a Word file was especially common in FY 2020.

Cybercrime in Instant Messaging cross-platform

They will ask you to keep their conversation secret

Scammers will try to contact you out of the blue. They pretend to be someone you know.



They will create such a situation that will seem like an urgency and will put you under pressure to respond quickly.

Fraudster will try to get your personal or financial details. The most recently case is sending the *apk file to deceive target to click. After clicking, the personal and financial details of target will be leak to fraudster.

BCA Mobile Apps – Virus on Pop Ups Application

- The latest viral alleged fraud mode in the BCA Mobile application is in the form of a pop-up notification with an appearance as if asking the user to remove the virus when they want to open BCA Mobile.
- This virus can cause devices to be accessed by remote applications without authorization. The fraud mode in the BCA Mobile application resembles the Android Package Kit (APK, file format .apk) mode.
- Hackers target the credentials (username and password) of financial data with the mission of controlling the target banking account.
- If the pop-up appears and is clicked, it says the .apk will automatically be installed and the user's cellphone is infiltrated by malware. Finally, user data can be owned by hackers.