CHECK!

For more secure communications on your smartphone…

Watch out for those emails and websites that have malintent!

They appear to be those from legitimate companies and try to take advantage of you. Please be updated about the most recent trends of cybercrime and stay cautious when you log onto the Internet.

Can the app you are installing really be trusted?

When you install an app, make sure that the app downloading site can be trusted and that you are not installing fraudulent ones. Also, you must be careful when you give any app permission to access your data.

Make sure that the operating system and apps that run on your mobile are the latest version!

Keep the OS and apps up-to-date, which will help prevent your device from being infected with viruses.

Deploy security software!

Smartphones should as well be protected by deploying anti-virus software as personal computers because those mobile devices also contain sensitive data.

MPD

dispatches information on cybercrime and cyber security.

情報セキュリティ広場 Search

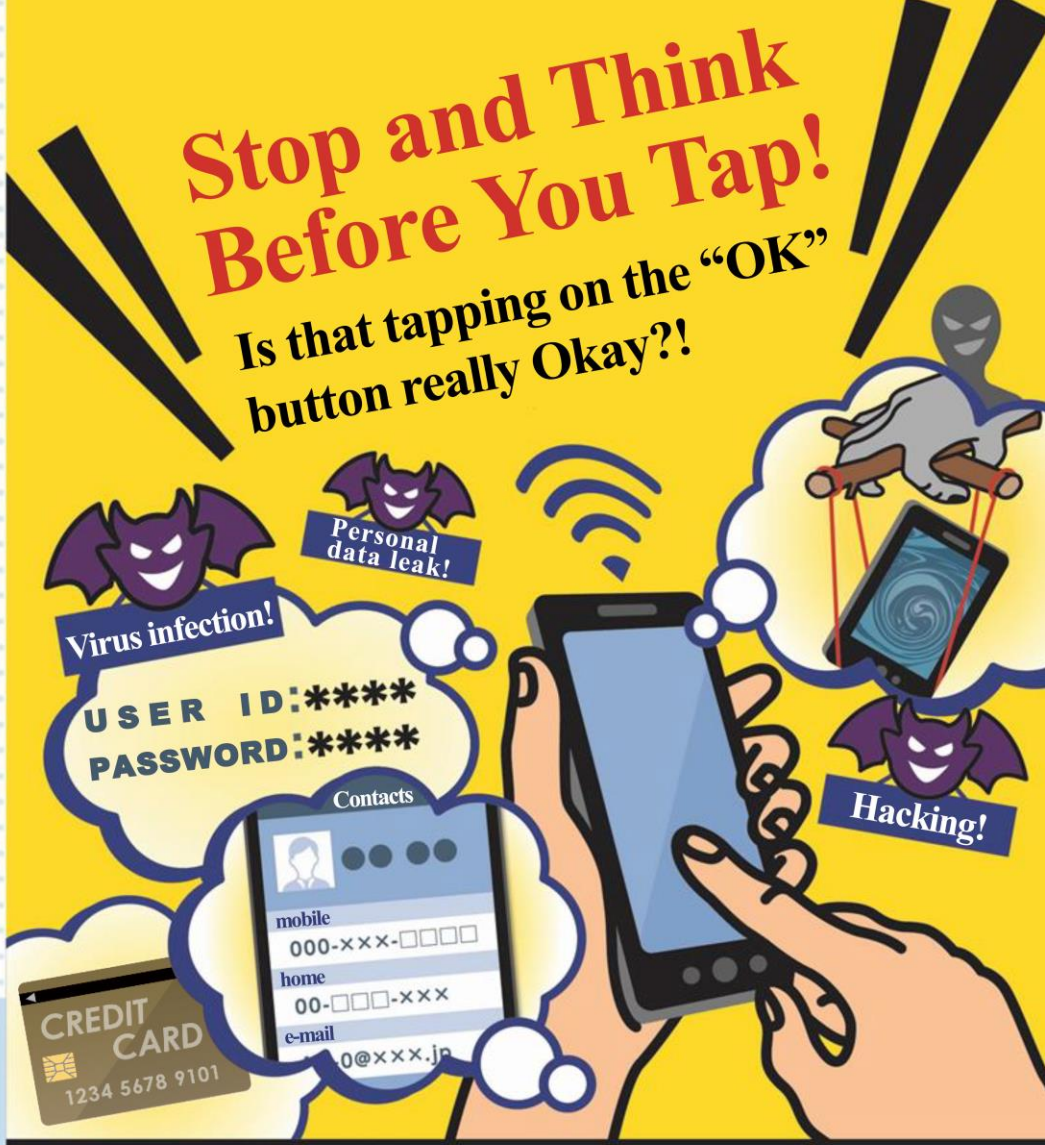
【Username】
@MPD_cybersec

MPD official YouTube channel

Cyber Security Control Task Force, Metropolitan Police Department

Stop and Think Before You Tap!

Is that tapping on the "OK" button really Okay?!



Take security precautions with your smartphone as well!

- Can the app you are installing really be trusted?
- Make sure that the operating system and apps on your mobile are the latest version!
- Deploy security software!

QR Code 情報セキュリティ広場 Search

街とともに、人とともに。
FOR MORE COMMUNICATION
けいしちょう

Stay cautious when using your mobile phone; otherwise…

CASE 1:

While checking out social network pages or a discussion board, or emails that have malicious intent, you are led to a web page, where you enter your credit card number or account user name and password, thus your personal data is stolen.

PHISHING scammers intercept your personal data:

Then the attacker abuses your information. They may steal your cryptocurrency or use your credit card, causing you financial damage.

CASE 2:

You click on the link in an email message you have received or open an attached file to it without thinking much about the consequences, only to have your computer infected with viruses.

RANSOMWARE-malicious programs demanding payment to recover access to your files or system:

Ransomware encrypts files stored on your system or locks the screen so you can no more use your file or system and then demands payment to restore access to them.

CASE 3:

You find an interesting app, but it turns out to be a malicious one.

HACKING:

Virus-infected apps can operate the camera or call recording feature of your mobile phone without your knowledge. They can also steal personal information, such as your contacts and calling history, stored on your smartphone.

Other Cases!

Photos you post on social media may unexpectedly become a cause of trouble!

- Location information and things caught in the background of a photo might be giving away information about the place you live in or the school you go to and you might fall victim to stalking…
- While travelling, you post a photo to your social media account and that might be telling someone that you are away from home, and your house might become a target for burglary or other crime…
- You post a photo with your friends in it without their permission and now any of you might be in trouble because of the post…

IMPORTANT: **Make sure that the photos you are posting are not carrying information leading to privacy concerns, such as location (GPS) information, places frequented by the people in the picture and their relations with each other.**

You click on the play button to view a streaming video and then a web page pops up, urging you to pay!

- You try to view a movie and click on a button and, all of a sudden, a web page appears showing you have signed up for membership, in some cases, with a loud camera shutter sound, making you feel further agitated, and then the web page urges you to pay…

IMPORTANT: **Stay cool and don't rush to pay nor contact them.**

While you are connected through a public Wi-Fi network, someone might be stealthily watching your online activity!

- Access to some public Wi-Fi networks is not properly secured and your online sessions might be stealthily being watched…
- In some cases, fake access points are set up with evil intentions…

IMPORTANT: **Transmission/reception of personal information, including credit card information, through public Wi-Fi networks is not recommended.**

Sharing the same password for login may lead to compromise your accounts on the web!

- Simple passwords might soon be cracked…
- If you are using the same password among several online services like e-commerce and once the password is accidentally disclosed, someone can sign in to your online accounts one after another and abuse your accounts and data without you knowing it…

IMPORTANT: **Set a different password for each different account. Those passwords should be created with upper/lower case letters, numbers and symbols mixed to avoid being broken easily.**