Recent Trends

Cybercrime with the intention of stealing money or information is on the rise.
Security software is not always perfect.
We can show you some more security tips worth practicing.

Public Wi-Fi hotspots

Some free Internet access points you may find in public places are not always properly secured for online communications and someone might be trying to see your online activity. Transmission/reception of credit card information or other personal data through public Wi-Fi networks is not recommended.

Trading goods/shopping online

Malicious e-commerce sites disguised as actual ones or with fake contact information are out there in great numbers and, even if you have made an order and a payment, you might not get what you ordered.
Some participants in online flea markets, auction sites or ticket marketplaces have malicious intent and may try to sell you things in a way you might later find unacceptable and, in some cases, don't even ship the goods you have already paid for.
Please make sure the bank details and contact information indicated on those sites can be trusted before you make any payment.

MPD dispatches information on cybercrime and cyber security.

情報セキュリティ広場 Search

Official Twitter account of Cyber Security Control Task Force, MPD

@MPD_cybersec

Cyber Security Control Task Force, Metropolitan Police Department

Is your online communication SE-CU-RE-D?

Cyber Security Notice from Metropolitan Police Department

SE…**SE**e that the download is safe!

CU…Keep the system **C**urrent and **U**p-to-date!

RE…**RE**view your password security!

D…**D**eploy security software!

Take security measures now!

Other Tips!

- Check out recent security developments!
- Back up important data!
- Be careful when posting on social media!

…and so on. Actually, there are lots of security tips readily available!

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

SE

SEe that the download is safe!

Personal computers and mobile devices are susceptible to computer viruses through malware or apps with malicious intent.
However convenient or interesting they may look, do not download files or apps that you cannot trust.

CU

Keep the system Current and Up-to-date!

In cybercrime, the attacker exploits vulnerabilities of your software or apps.
To close security holes, update your system immediately after the latest version of security patches is issued.

RE

REview your password security!

If several accounts share the same User name or Password and once those secret codes are cracked, then they can be used by someone to sign in to one account after another with malicious intent.
Set a different password for each different account and it is important you have control on them. One way could be to keep the passwords on your pocket diary or notebook.

D

Deploy security software!

Despite all your efforts, computer viruses are lurking right behind your system waiting for an opportunity to infect your computer.
Anti-virus software helps protect the personal data on your personal computer and mobile devices from computer viruses.

Other Security Tips!

Stay current with the latest cyber security developments!

With the wide spread of smartphones, a great number of people now use the Internet every day and anyone can fall victim to cybercrime.
We are seeing victims of ransomware worldwide and cybercrime is evolving day by day.
To protect yourself against cybercrime, please be updated about recent cyber security topics and take precautions against the crime online.

It's worth backing up your data regularly!

Your data can be destroyed due to various factors, such as disasters, computer glitches, unintended operation and computer viruses, and it is hard to protect your data from all those unwelcome events.
Once data is broken, it cannot be recovered.
It is recommended that important data has a backup copy in case of an unexpected event.

Is your social media post all right?

Certainly, social media is a powerful communication tool, but your post might cause a negative response in ways you had not even imagined.
To avoid any trouble, keep in mind that anyone can see whatever you say or show on social media. Pay enough attention to the posts you are making.

If you will, you can practice any of the above security precautions right now.

"SECURED" doesn't always mean "PERFECT".

You can never be careful enough! Keep in mind that the action on your part counts if you are to protect your data.