'15 DISI

INTERNATIONAL COMPUTER
SECURITY DAY

Staying safe
in an increasingly
mobile world

disi.rnp.br

CAIS

RNP

About the **event**

The International Computer Security Day (Disi) has been held since 2005 by the Brazilian National Research and Educational Network (RNP), through its Security Incident Response Center (CAIS), in partnership with the Organization of American States (OAS) and the Latin American Cooperation of Advanced Networks (RedCLARA).

Held annually, the event brings together experts on information security to share their knowledge and thus educate and train internet users.

At every edition of the event, the organization chooses a theme to direct the activities of Disi. This year, discussions will be carried out based on the theme **"Staying safe in an increasingly mobile world."**

Among awareness activities particularly elaborated for Disi, one finds speeches on information security, on-site and broadcasted in three languages (Portuguese, Spanish and English), in addition to the publication of awareness material on the website and distribution of the material at the event.

Security tips

Use different passwords on your email, social networks and other online services. If any of your passwords is violated, the other will be protected. Additionally, always try to define “strong” passwords and change them periodically.

Making use of an infected computer for online purchases can cause someone to steal your credit card number or other sensitive information. **To reduce this risk, use an up to date antivirus software on your computer.**

Cell phones and tablets can also be infected! **Check at the RNP website the booklet “Security in Mobile Devices” and be safe.**

Make back up regularly of your documents, photos and other important data stored on computers and devices that you use in your daily basis. Do not wait for a sudden loss of data to happen in order to care about them.

Keep your computer's software and mobile and tablet apps updated. Remember that updates are essential to protect the systems and data.

Set up a custom password for the wireless router at your home because the factory default password can be easily identified by third parties and your network will be unprotected. When setting the router, use the WPA2 protocol as the safest option to protect your network.

Try not to share personal data and sensitive information on your social networks. Also be careful not to expose third parties without permission. This applies particularly to underage children.

Never click on suspicious links arriving by email, social networking and chat services. Suspect of emails requesting bank data update, information of your award-winning lottery ticket or any other message requesting personal data or sensitive information – these messages are often fraudulent.

Watch out for the physical security of your information: do not leave papers with sensitive information on the office desk, such as passwords written on post its.

Take care also about private conversations in public places to prevent the leakage of information without intending to disclose it.

Security tips

Mobile devices

Use unique passwords for each online service you use. Ideally, each password must have a high level of complexity to prevent its discovery by others.

Some online services offer more than one type of authentication, matching password and sending SMS code, for example. Make sure the used service offers that alternative and, if possible, choose to have two authentication criteria. Therefore, your account will be more protected.

Confidential files should be stored safely. Encryption can help in this regard. Some online services now offer this service automatically, but if not, the ideal is you encrypting you own files.

Avoid using open Wi-Fi networks – those with no password, commonly available in airports and cyber cafés – particularly when transmitting sensitive data. Examples include banking applications and websites purchasing.

Before disposing of a mobile device, always remember to remove the data and device settings so these data do not reach third parties.

Synchronize contacts and calendar from your smartphone or tablet. This way you will not loose your contacts in case of loss, theft or even device failure.

Install apps only from official sources that guarantee the origin of the applications. For Android use Google Play, for Apple use App Store and for Windows use Windows Store.

We know it's useful and practical keeping passwords saved in its own applications, but with this you are at risk. Once the device is lost, stolen/robbed or misplaced, a third party could, for instance, have direct access to your social networks. If you do not give up on this facility, it is recommended an application that allows to erase all data remotely.

Have fun **safely**

MOBILITY
PRIVACY
APPLICATION
SMARTPHONE
TABLET
SECURITY
INFORMATION
TERMS OF USE
EMAIL
NOMOPHOBIA

S H Y M N T B H M P N B R P O I R A E E
P O L T E A S E C U R I T Y C Y R I N I
M V A H I B O O V M P O H B P P T N O S
M C S T E L P R R V P Y N E B L I F M R
T E M M S E I C M V C C O P V B E O O Y
E N N H R T V B Y E S A I V C S H R P I
R M L O Y O N N O I C V T M A T R M H H
L E R T H O T P L M B I A S B H H A O T
E B L L H P A A R S M R C L R C L T B V
O T B M H A T A Y E E P I C P B O I I M
M A B N B R S R O M I R L S E R S O A N
A A O Y S L V N A R H H P N P V A N A R
A H I H T E R I V M V L P T R B T S V C
E E O T V H L M C S S V A R C I B M B L
I P H R S P M V I I L R S I O V L H N A
I R N Y Y R L C V Y T A C P M S B P R B
E B E E T R Y C S H N Y B M B S O R R O
L S T E R M S O F U S E O S P T H C V L
U N L V L A I P H C V M Y I O B N S Y Y
V I B H O Y T Y A A N B R O I V V C N L

Learn more about some security services of RNP for the internet community

Security alerts:

http://www.rnp.br/servicos/seguranca/educacao-e-conscientizacao-seguranca

Network Time Synchronization:

ntp.cais.rnp.br

Fraud catalogue:

http://www.rnp.br/servicos/seguranca/catalogo-fraudes

You can contribute with this service, forwarding:

fraudulent e-mails to phishing@cais.rnp.br

Emails containing attached malware or links to artefatos@cais.rnp.br

More **information**

CAIS | Security Incident Response Center

http://www.rnp.br/servicos/seguranca

DISI | International Computer Security Day

http://disi.rnp.br

Security Month

http://meseg.rnp.br

'15 DISI

INTERNATIONAL COMPUTER
SECURITY DAY

Sponsorship

GRUPO BINÁRIO
Integração | Serviços | Mobilidade

JUNIPER NETWORKS

HUAWEI

Ruckus
Simply Better Wireless.

Support

POP-DF

UnB

Escola Superior de Redes RNP

10 anos

Partnership

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

RedCLARA
+ Red + Ciencia

Organization

CAIS

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL
BRASIL
PÁTRIA EDUCADORA