IT Security Measures

Definition & Goals

What is IT Security?

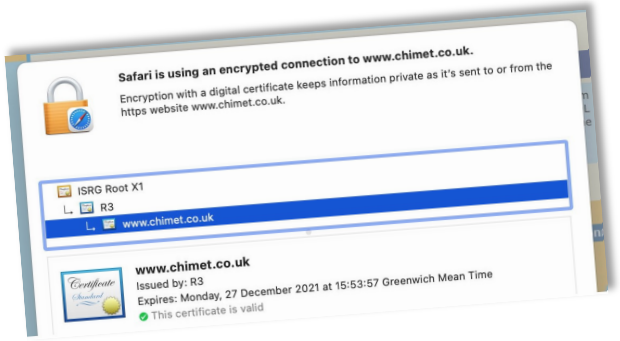
- IT Security is a set of cyber security strategies that prevent unauthorized access to company resources such as computers, networks and data.

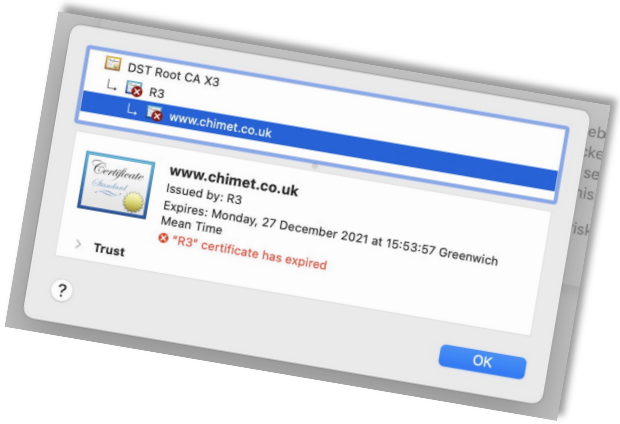
What is the goal of IT Security Measures?

- Achieve sufficient and appropriate IT security at Nanjing University

General Safety Measures (1)

- Regular **updates**
  - Antivirus programme
  - Web browser
  - Operating System





- Regular installation of all available **safety updates**
  - Operating system (e.g. Microsoft, MAC OS/iOS, Android, etc.)
  - Programmes (e.g. web browser, office, etc.)
- **Software and programmes** should only be obtained from **trustworthy sources**
  - Websites of the software manufacturers
- Surfing is most secure with an **encrypted connection (https)**
- Ensure that the **certificate** is **valid and trustworthy**
  - Digital certificates certify the trustworthiness of communication partners on the Internet

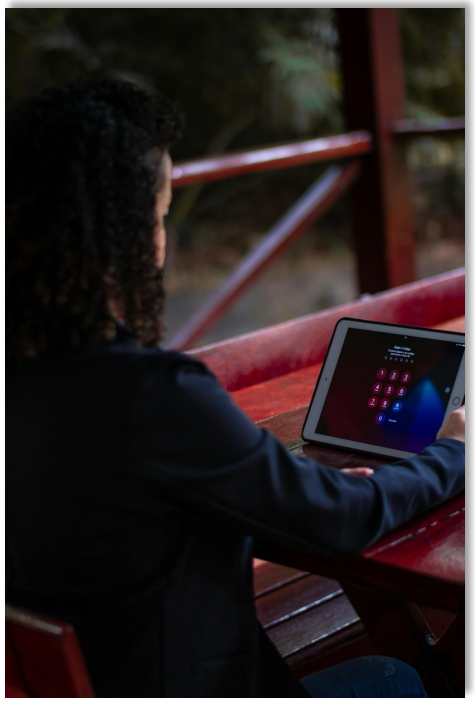
General Safety Measures (2)

- Do not automatically click on links or file attachments sent by email
  - Always consider first whether the attachment and content are reasonable
- **Wi-Fi connections** should not be used without thought, as they do not always provide a safe, **encrypted connection**. Especially when dealing with **sensitive data** (e.g. online banking, shopping, etc.), an encrypted connection is essential
- The Nanjing University unified identity authentication account cannot be rented, loaned, bought, sold, given away, or otherwise transferred to anyone else. If you have security issues, please directly contact the faculty or the Information Technology Service Center for assistance
  - **Information Technology Service Center website:** https://itsc.nju.edu.cn/itsc_en/main.htm

Safe Passwords

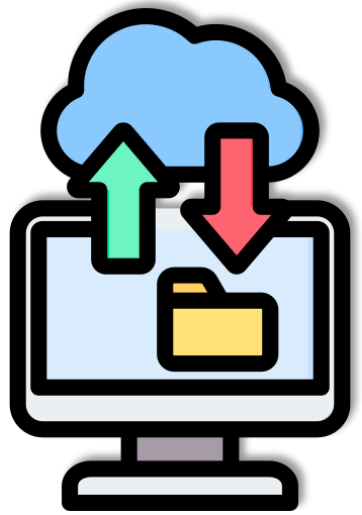
Use strong passwords:

- At least 10 characters (a password length of 16 characters is recommended)
- The password should consist of upper- and lower-case letters as well as special characters and numbers
- Do not use old passwords
- The password should be kept secret and changed regularly
- Company passwords should not be used for external services



Data Backup

- Users should only store their important data on the home drive or on the group drives (if available)
- All data on the file servers of the University Computer Centre are backed up daily by the central backup service
- Regular data backup to at least one external storage medium (two storage mediums are recommended)
- A complete data backup not only backs up data and documents, but also programmes and the operating system



Safe Use of Email Services

- Business email addresses should not be used for private external services (e.g. social networks, online shopping, etc.)
- For security reasons, students are advised to use their university email accounts for electronic communication with members of the university
- Contaminated email attachments and links are one of the most common ways of infiltrating computers with malware. For this reason, you should always pay close attention before clicking on a link or opening an attachment. The sender, subject and email text should be consistent and reasonable
- Digital certificates certify the trustworthiness of communication partners. Pay attention to the validity and trustworthiness of the certificate when you receive a signed email

Social Engineering

What is Social Engineering?

- In social engineering, human characteristics such as helpfulness, trust, fear or respect for authority are exploited to cleverly manipulate people. In this way, the attackers trick the victims, for example to give away confidential information

Protective measures against social engineering:

- Use social networks responsibly. Think carefully what personal information you publish there, as this information can be collected by criminals and misused in attempts to deceive you
- Do not disclose confidential information about your work in private and professional social networks
- Never share passwords, access data or account information by phone or email. Banks and companies never ask their customers to share information by email or telephone
- Be particularly careful with emails from unknown senders
- If a response is absolutely necessary, call the sender to make sure that it is a legitimate email

Malware (1)

What is Malware?

- Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems
- Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware

Types of Malware

- **Virus:**
  - Deletion of or damage to information, data and systems
- **Trojan viruses:**
  - Extortion
  - Spying and recording (keystrokes, microphone and webcam)
  - Misuse of systems and devices for illegal activities

Malware (2)

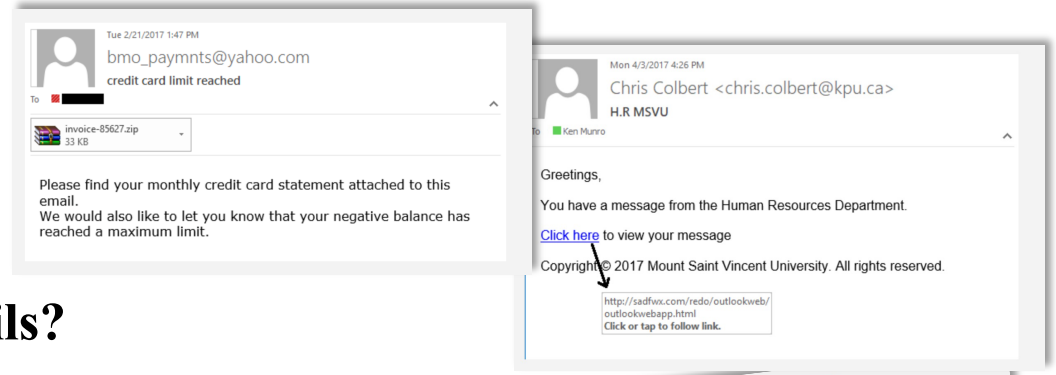
How does Malware spread?

- Opening contaminated email attachments
- Spam & Phishing emails with disguised links
- Opening damaged websites
- Execution of infected files/downloads

Phishing & Spam Mails (1)

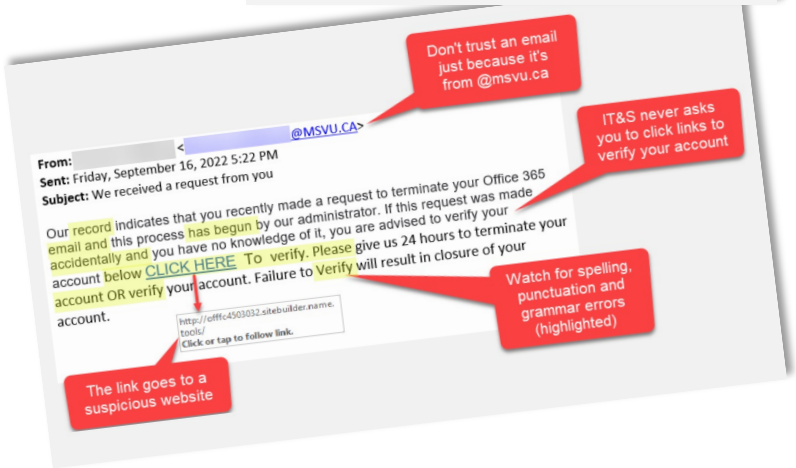
What are Phishing Mails?

- Unwanted emails that contain Malware



How do you recognize Phishing & Spam Mails?

- Sender addresses are fake
- Confidential data is requested
- Urgent need for action is signalized
- Misspellings are present
- The emails contain links that should be opened by the receiver



How to prevent phishing?

- Strict password management policies. For example, you should change your passwords frequently and should not reuse a password for multiple applications
- Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications

Phishing & Spam Mails (2)

Guideline on how to identify phishing emails:

- Most phishing emails are automatically blocked by the school email system, but for the few that slip through the net, we need to take protective measures

1. Fraudulent emails with fake leader names

- Check the sender information of this type of email. You can see that it is an unknown email address and it's not a Nanjing University email address.

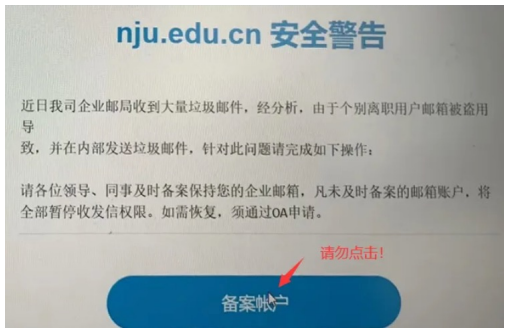
- The content of similar phishing emails is “I can't talk right now, help me transfer my money.”, “Click a link for me, vote for me.” and other common fraudulent phrases. **Please do not believe the messages and do not click on the links!**

Phishing & Spam Mails (3)

2. Fraudulent emails that appear to be system notices (1/2)

- The sender's address is not the email address of Nanjing University, nor is it Tencent's customer service e-mail address, therefore, it is a fraudulent e-mail

- More confusing phishing emails fake the sender's address as a Nanjing University email address. Such emails with fake addresses are usually automatically blocked by the system
- If a Nanjing University student receives this kind of email, especially those blocked by the system and sent to the spam folder, please do not believe it. Do not click on it and do not enter your password



Phishing & Spam Mails (4)

2. Fraudulent emails that appear to be system notices (2/2)

- **Warm tip**: Tencent system mailbox notification has “anti-counterfeiting mark”. When you open the email on the web, you can see the small blue icon

- In addition to the upgrade reminder sent by the Information Technology Center, the email will include an on-campus phone number for you to call to check on the situation
- You can also visit the Information Technology Center website (http://itsc.nju.edu.cn) to verify the notice

Phishing & Spam Mails (5)

3. Notices from fake off-campus institutions

- If an NJU member receives such an email, please confirm it through official channels. Do not trust them

How can I protect myself from phishing emails?

- If we come across suspicious emails, we should follow the principle of the "three don'ts": **do not reply, do not click, do not download**
- For emails that turn out to be phishing emails, you can report them directly. This allows the system to learn from additional data and optimize the blocking mechanism
- If you are not sure if it is a phishing email, you can forward the email to us at mailreport@nju.edu.cn or call the appropriate department to make sure.
- **Warm tip**: If the email does not contain the telephone number of the university office, please take precautions

Phishing & Spam Mails (6)

What if I have already replied to or clicked on a phishing email?

1. If you have clicked on a link or downloaded something within the phishing mail, please remove the virus on your computer or mobile phone
2. If you have provided personal information, please change your account password immediately

- You can also send an e-mail to mailreport@nju.edu.cn and ask for further information to prevent the loss of personal information or money
- Students and teachers should be aware of the following: If you come across suspicious email, please do not reply, click or download. Forward them to mailreport@nju.edu.cn for advice or call 025-89683791 by phone. Seek support and help when it is needed!

- ***Let's raise awareness for prevention!***
- ***Let's not allow ourselves to be exploited by phishing emails!***