Reminder for users

Did you receive an email and don't know how to tell if it's genuine? This is not always easy to do, pay attention to the details of the message.

> The technical service of the university never asks for a username and password from your account. If you have received a suspicious message and you doubt its safety, you can always write (*4141@nsu.ru*) or call (363-4141) the NSU user support service and ask your question.

Information about the sender. It is impossible to determine the authenticity of a message only by the sender. Attackers can specify any Information in an e-mail message, including the sender, so that it looks more like an official one. As a rule, companies with a good reputation do not use public email services, such as Gmail, Yandex or Mail.ru. In order to check the email from which the letter was sent, you need to hover over its name (in the example - "Zimbra Administrator", mail zimbra@mail.ru, here you should pay attention to the mail.ru domain, any letters from technical support should come from the domain nsu.ru, usually this is a mailbox - support@nsu.ru).

Be aware of this possible trap.

Subject Line – Senders, whether legitimate companies or scammers, often use catchy phrases as subject lines to grab attention.

Logos and Names - Many email messages use company logos and first names. Attackers can spoof these elements, so don't judge the security of an email by them.

Links - Examine the link carefully, this can help determine if the website the link leads to is genuine or a scam. Often, attackers use domains that are very similar to the official ones, but if you look closely, you can see a set of different characters, or a part that looks like the official domain is at the end or middle of the link.

> Emails may contain malicious links, by clicking on which you will give attackers full access to all your data. Access to confidential data - passwords, accounts, financial data - will allow hackers not only to delete or make your data publicly available, but also to use financial tools such as mobile banking, payment systems, and money transfers on your behalf.

Follow only those links that are probably safe.

Signatures and Contact Information – Reliable, authentic contact information is easy to verify. Always check that phone numbers are correct before calling service centers.

Grammar and Spelling Errors - Pay attention to sentence structure as well as spelling errors, legit companies usually don't make these kinds of mistakes.

Requests for important information - Beware of requests or confirmation of important information. Remember - law-abiding companies will never ask you to enter your username and password anywhere.

Urgency - Attackers love to use this trap to force you to act quickly without thinking.

Attached files - before opening a file, carefully study the letter in which it is attached. Very often, attackers send files containing a virus that encrypts all the information on your computer. The message is disguised as official correspondence (report, act, request, invoice, etc.), while often not personalized to the owner of the box and impersonal. Often such letters have a zip, rar ATTACHMENT containing a file in JS, SCR, EXE, COM, VBS formats (any non-standard for office workflow). Example: "Reports.zip", and inside "Reports.scr".

When you try to open such files, the expected launch of office programs (word, excel, etc.) does not occur, and the machine becomes infected.

In no case DO NOT try to open them on the computers of friends, colleagues, or neighboring departments! DO NOT AGREE to the requests "I DID NOT OPEN, TRY IT AT YOURSELF"! In case of infection - you should immediately turn off the computer and call NSU technical support to prevent the spread of infection at the initial stage.

> And remember: if you receive a suspicious message and you doubt its safety, you can always write (*4141@nsu.ru*) or call (363-4141) the NSU user support service and ask your question.

Recommendation: To protect your computer, install Kaspersky Anti-Virus -*Инструкция по настройке антивируса Kaspersky Endpoint Security*