Users Guideline for NUST o365 Security

It seems that the user password is compromised, and his/her account is sending suspicious messages regularly. For a quick action following actions are taken:

1. **Multi-factor Authentication enable (after confirmation received from user end)**
2. **User password is reset (in case of student change from on-prem AD & wait for Sync)**

User are advised to change his/her password immediately and password should be complex containing at **least 8 characters long**. Along with **upper and lower-case characters**, require multiple occurrences of **digits and special symbols**. Such passwords provide strong protection from brute-force attacks.

User must follow the following instructions during changing the password:

1. THINGS TO INCLUDE

1. At least eight characters.
2. One or more of each of the following:
   a) lower-case letter
   b) upper-case letter
   c) number
   d) punctuation mark
3. Lookalike characters to protect against password glimpses. Examples:
   a) O as in Oscar and the number 0.
   b) Lower-case l and upper-case I.
   c) The letter S and the $ sign.

2. THINGS TO AVOID

1. Words he/she can find in the dictionary.
2. Passwords shown as "example strong passwords."
3. Personal information, such as names and birth dates.
4. Keyboard patterns, like qwerty or 12345. Particularly avoid sequences of numbers in order.
5. Common acronyms.
6. All one type of character - such as all numbers, all upper-case letters, all lower-case letters, etc.
7. Repeating characters, such as mmmm3333.

3. MEMORABLE PASSWORD TIPS

While passwords that are easy for user to remember are also less secure than a completely random password, following these tips can help you find the right balance between convenience for his/her and difficulty for hackers.

1. Create a unique acronym for a sentence or phrase you like.
2. Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh.'
3. Jumble together some pronounceable syllables, such as 'iv,mockRek9.'

4. KEEP PASSWORD SECRET

1. Never tell your password to anyone (this includes significant others, roommates, co-workers, etc.). If you need to grant someone access to your server, set up a separate username and password for that person.
2. Never write your password down, especially not anywhere near your computer.
3. Do not store your password in a plain text file on your computer.
4. Never send your password over an unencrypted connection - including unencrypted email.
5. Periodically test your current password.
6. Update your password at least every six months.

5. Users are also advised please don’t open unknown sender email or irrelevant email. If you suspect that you have clicked on a malicious attachment or suspicious link:

1. Immediately disconnect the computer from the internet.
2. Scan your machine with up-to-date Anti-Virus software.
3. Do not input any sensitive information into the machine until the Anti-Virus scan is passed.

6. Follow below guidelines to avoid any threat to his/her computer:

1. Treat messages from an unknown sender with extreme caution.
2. Never open, run or save attachments from unknown Senders - this is what normally carries the Trojan software.
3. Don't click on any link in an e-mail from a user or organization unfamiliar to you asking to upgrade your mailbox or request for any secure information such as password etc.
4. Don't respond to any request via e-mail to pass on any "secure" information about yourself, for example user IDs and passwords.
5. Don't run or save attachments to e-mails apparently sent by legitimate organizations where you have not solicited the e-mail. Check to company web site or call to confirm the message is trustworthy.
6. Keep your computer up-to-date with latest anti-virus software and keep it on auto update.

In line with good computing practice, recipient should keep in mind above mentioned guidelines in order to minimize risk of virus attacks on your computer.

Regards,

NUST O365 Support Team