INFORMATION SECURITY

Next

PASSWORDS

- Create a strong password that is at least twelve characters long. Do not use your name or family member's name in the password. Your password should contain at least two of the following four categories:

  * Uppercase letters
  * Lowercase letters
  * Numbers
  * Special characters

- Change your password immediately and contact the help desk at ext. 1560 if you suspect that your password has been compromised.
- Do not write your password down on paper or store it in an unencrypted computer file.
- Do not send user names and passwords in emails that are not encrypted.
- Do not use the "Remember Password" feature that may be available in an application or website.

NEVER SHARE YOUR PASSWORD!!!

- Do not share your password with anyone!!! That includes anyone in the IT department/Help Desk.

- Any employee found to have shared a password may be subject to disciplinary action, up to and including termination of employment.

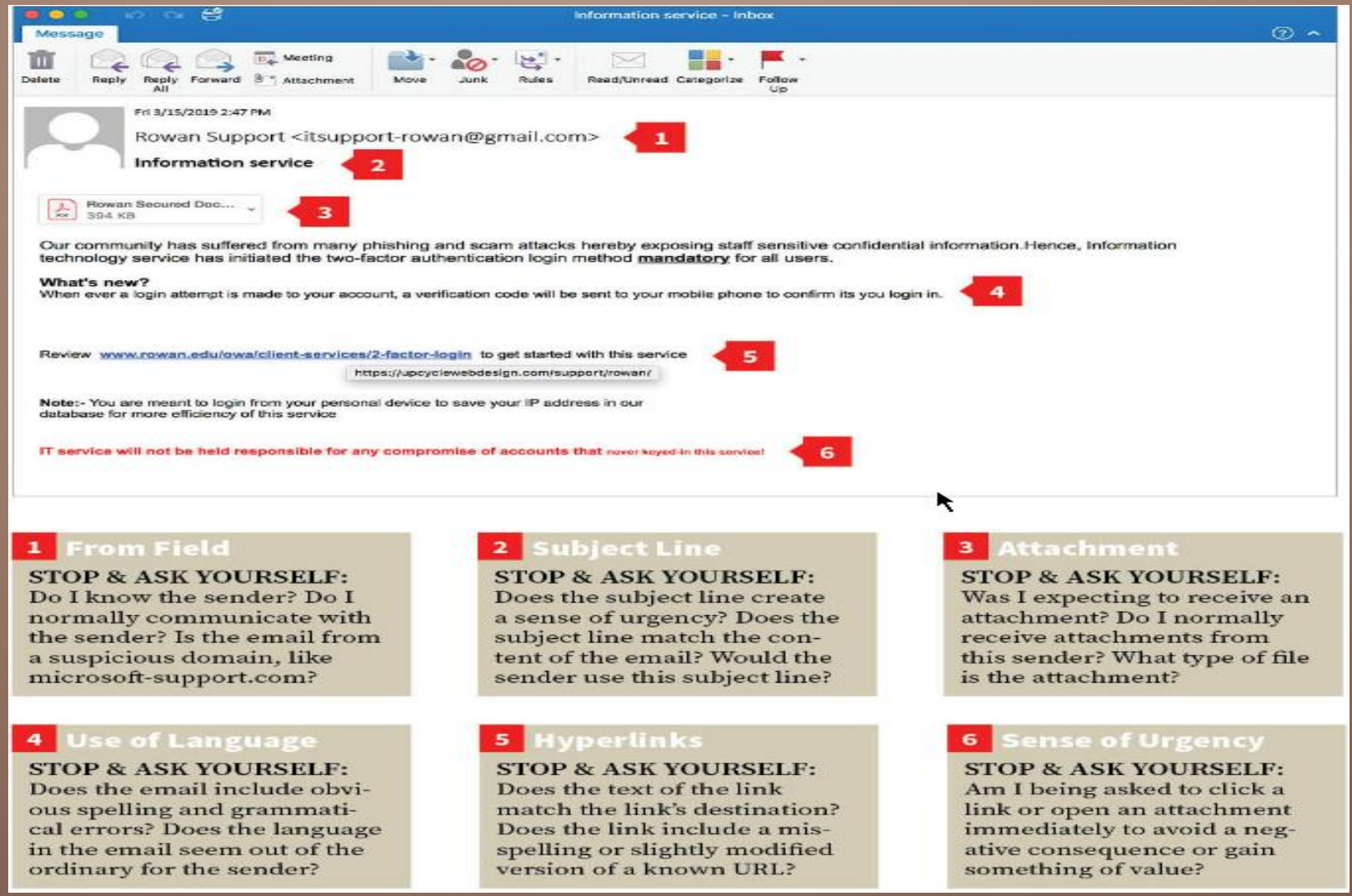
DESKTOP/LAPTOP COMPUTER

- Log off, disconnect your session, or lock the computer every time you step away.
- Do not save any confidential information on the C-drive (local drive) of your computer. Save important and confidential data in your P-drive. Your P-drive is backed up regularly by the IT department.
- Installing software is prohibited unless the software has been approved and installed by the IT department.
- The use of USB devices such as flash drives, hard drives, CD/DVD burners, and cameras are prohibited unless they have been approved by the IT Department to support patient care.

EMAIL SECURITY

- Do not send confidential information in an email unless it is required as part of your job. Email messages with confidential information must be encrypted. Messages can be easily encrypted by typing ***encrypt*** anywhere in the subject line of the email.
- Do not open attachments or links from an unknown sender. Be very cautious as phishing emails are intentionally designed to look very real and may even contain an organization's logo and trademark.

HOW TO SPOT A PHISHING EMAIL



Previous

Next

REMOTE ACCESS

Follow these guidelines if you remotely connect to MCH applications:

- Disconnect the remote session every time you step away from the computer.
- The computer being used to connect remotely to the MCH network must have up-to-date anti-virus and anti-spyware software installed.
- Never save any MCH Information on your personal devices such as laptops, desktops, flash drives, CDs, etc.
- Do not connect to the MCH network from a public place.

THANK YOU!

Thank you for taking the time to review this information.

Our priority is to protect both you and our patients at all times.

CONTACT INFORMATION

Issue	Contact
HIPAA Security questions	**IT Help Desk, Ext 1560**
Report a HIPAA Privacy violation, compliance questions, or concerns	**Compliance Hotline 1-800-826-6762**
Report an Information Security violation or any Information Security concerns	**IT Help Desk at Ext 1560**
Dispose of electronic media (computers, hard drives, laptops etc.)	**IT Help Desk, Ext 1560**
Report a lost ID Badge	**Human Resources, Ext 1585**
Ask an email security question	**IT Help Desk, Ext 1560**
Report a lost or stolen laptop computer	**IT Help Desk, Ext 1560**
Report a lost or stolen Blackberry phone or other smart phone	**IT Help Desk, Ext 1560**

Previous