International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 5 Issue 1, January - 2021, Pages: 36-40

Organization of E-Mail Protection

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Email or E-mail is the most popular part of the Internet use process today. You can instantly send or receive emails anywhere in the world, and send emails not just to one person, but to a list of addresses. There is an opportunity to discuss via e-mail, and in this direction the USENET server is gray.*

Keywords: USENET, SMTP, POP, IMAP, MIME.

INTRODUCTION

1. Use of e-mail

2. Basics of e-mail

3. Existing problems in e-mail

4. Risks present in e-mail

5. Email protection

Use of e-mail

Email or E-mail is the most popular profession in the process of using the Internet today. You can instantly send or receive emails anywhere in the world, and send emails not just to one person, but to a list of addresses. There is an opportunity to discuss via e-mail, and in this direction the USENET server is gray.

Many companies use the e-mail system directly in their business. This means that business leaders need to take certain measures to teach their employees to work with e-mail and use it wisely. The main purpose of this process is to set the right course for working with important documents.

METHODS

Here it is necessary to take into account the proposals in the following areas:

- Use of e-mail system for organizational purposes;

- use for personal purposes;

- Storage and access to confidential information:

- Save and manage emails.

Basics of e-mail

The main postal protocols on the Internet include:

- SMTP (Simple Mail Transfer Protocol);

- POP (Post Office Protocol);

- IMAP (Internet Mail Access Protocol);

• MIME (Multi purpose Internet Mail Extensions).

Let's get acquainted with them one by one:

SMTP - based on this protocol, the server receives messages from other systems and stores them in the user's mailbox. Users with interactive access to the mail server can read messages directly from their computers. Users on other systems can read Facebook messages via ROR-3 and IMAP protocols;

POP is the most common protocol, allowing messages on the server to be read directly by the user, even if they are received from other servers. Users can view all messages or messages that have not been read yet. Currently working on version 3 of POP

logged out and enriched with authentication methods;

IMAP is a new and therefore less common protocol.

This protocol has the following capabilities:

• create, delete and rename mailboxes;

• arrival of new letters;

• fast sending of letters;

• search for letters; • Select messages.

IMAR is more convenient than POP for traveling users;

MIME is an acronym for multi-purpose Internet mail that allows you to specify the format of messages, namely:

• sending texts in different encodings;

• sending anonymous information in various formats;

• the message consists of several parts;

• Include information in various codings in the subject line.

This protocol consists of digital electronic signatures and data encryption tools, which can also be used to send executable files by mail. As a result, it is possible to spread viruses along with files.

Problems with e-mail

The following mistakes can be made when working with email:

• accidental sending of a letter;

• the letter was sent to the wrong address;

• system failure due to a sharp increase in mail archives;

• incorrect subscription to news;

• Make a mistake in the mailing list.

If the organization's mail system is directly connected to the Internet, the consequences of errors will increase dramatically.

Here are some ways to prevent these errors:

- user training;

- Proper configuration of e-mail programs;

- Use software that fully complies with Internet protocols.

In addition, the use of e-mail for personal purposes can cause some problems for the management of the organization, as it is possible that the e-mail address will contain the names of the organization. As a result, the letter sent by the person can be considered as on behalf of the organization. Therefore, it is necessary to limit the use of e-mail for personal purposes, such as phones. Of course, this is a difficult issue to implement.

Risks in e-mail

There are the following risks when working with email:

1. The sender's fake address. Accepted letter It is difficult to be sure of the accuracy of an email address, as the sender may falsify the Google address.

2. Get the letter. The e-mail and its title are sent without modification or encryption. Therefore, it can be reduced to ashes on the road and change its content.

3. Mail "bomb" si. Many e-mails are sent to the mail system, and as a result, the system crashes. Mail server crashes are:

• The disc is full and subsequent messages will not be accepted. If the disk is systemic, then the system may crash completely;

• As a result of the increase in the number of letters in the queue at the entrance, subsequent letters are not queued at all;

• as a result of changing the maximum number of received letters, subsequent letters will not be accepted or deleted;

• As a result of filling the disk allocated to the user, subsequent messages will not be accepted and the disk will not be cleared.

4. "Scary" (unpleasant) letter. Emails received over the Internet may be sent by unknown individuals and may contain words that may offend users.

Email protection

The following methods of protection against the above hazards have been developed:

- Fake address protection, in which case it is recommended to use encrypted electronic signatures;

- protection against message capture, in which case it is recommended to encrypt the message or sending channel.

These protection methods directly reduce the share of remaining risks.

RESULTS

1. The sender's fake address. Accepted letter It is difficult to be sure of the accuracy of an email address, as the sender may falsify the Google address.

2. Get the letter. The e-mail and its title are sent without modification or encryption. Therefore, it can be reduced to ashes on the road and change its content.

3. Mail "bomb" si. Many e-mails are sent to the mail system, and as a result, the system crashes. Mail server crashes are:

• The disc is full and subsequent messages will not be accepted. If the disk is systemic, then the system may crash completely;

• As a result of the increase in the number of letters in the queue at the entrance, subsequent letters are not queued at all;

• as a result of changing the maximum number of received letters, subsequent letters will not be accepted or deleted;

• As a result of filling the disk allocated to the user, subsequent messages will not be accepted and the disk will not be cleared.

4. "Scary" (unpleasant) letter. Emails received over the Internet may be sent by unknown individuals and may contain words that may offend users.

DISCUSSION

Let's get acquainted with them one by one:

SMTP - based on this protocol, the server receives messages from other systems and stores them in the user's mailbox. Users with interactive access to the mail server can read messages directly from their computers. Users on other systems can read Facebook messages via ROR-3 and IMAP protocols;

POP is the most common protocol, allowing messages on the server to be read directly by the user, even if they are received from other servers. Users can view all messages or messages that have not been read yet. Currently working on version 3 of POP

logged out and enriched with authentication methods;

IMAP is a new and therefore less common protocol.

This protocol has the following capabilities:

• create, delete and rename mailboxes;

• arrival of new letters;

• fast sending of letters;

• search for letters; • Select messages.

IMAR is more convenient than POP for traveling users;

MIME is an acronym for multi-purpose Internet mail that allows you to specify the format of messages, namely:

• sending texts in different encodings;

• sending anonymous information in various formats;

• the message consists of several parts;

• Include information in various codings in the subject line.

This protocol consists of digital electronic signatures and data encryption tools, which can also be used to send executable files by mail. As a result, it is possible to spread viruses along with files.

Problems with e-mail

The following mistakes can be made when working with email:

• accidental sending of a letter;

• the letter was sent to the wrong address;

• system failure due to a sharp increase in mail archives;

• incorrect subscription to news;

• Make a mistake in the mailing list.

CONCLUSION

In addition, the use of e-mail for personal purposes can cause some problems for the management of the organization, as it is possible that the e-mail address will contain the names of the organization. As a result, the letter sent by the person can be considered as on behalf of the organization. Therefore, it is necessary to limit the use of e-mail for personal purposes, such as phones. Of course, this is a difficult issue to implement.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.