**Міністерство освіти і науки України**

**Національний авіаційний університет**

Навчально-науковий інститут аеронавігації, електроніки та телекомунікацій

#### Кафедра авіаційної англійської мови

**КОНСПЕКТ** **ПРАКТИЧНИХ ЗАНЯТЬ**

з дисципліни «**Іноземна мова за професійним спрямуванням»**

**Галузь знань:** 17 «Електроніка і телекомунікації»

**Спеціальність:** 172 «Телекомунікації та радіотехніка»

**Спеціалізація**: «Телекомунікаційні системи та мережі»

Укладач: Король Л.П.

Конспект практичних занять розглянутий та схвалений на засіданні кафедри авіаційної англійської мови

Протокол № 6 від « 18 » травня 2018р.

Завідувач кафедри д.п.н. \_\_\_\_\_ Пазюра Н.В.

**Module I** **HISTORY OF THE INTERNET**

 1 THE INTERNET – WHAT IS IT?

2STRUCTURE OF THE INTERNET

3IP ADDRESSES

4 SNEAKY WAYS TO GET AROUND THOSE INTERNET PRIVACY ISSUES

 5 PRIVACY WHILE BROWSING THE WEB

6 WEBSITE PRIVACY POLICY

**Module II.** **INTERNET SERVICES**

1 INTERNET PROTOCOL SUITE

2 FILE TRANSFER PROTOCOL

3 THREE WAYS TO MAKE SURE YOUR ONLINE CREDIT CARD TRANSACTION IS SAFE

4 PUBLIC KEY CRYPTOGRAPHY

5 DECIPHERING INTERNET E-MAIL

6 E-MAIL PROTOCOLS

**Module I**

 **HISTORY OF THE INTERNET**

 **THE INTERNET – WHAT IS IT?**

The Internet is an international computer network that provides users with access to information stored on thousands of different computer systems that tie together millions of different computers. Different systems are able to communicate with each other using TCP/IP, a set of protocols that defines how computers exchange information with each other.

The Internet had its foundation in 1969 with the development of the ARPANET (Advanced Research Projects Agency Network), a Department of Defense funded project designed to develop and test networking technology. Originally hosted by four research universities in the United States, the project was later expanded to include other computer systems in the United States, England, and Norway. By 1983, DARPA (Defense Advanced Research Projects Agency) had decided on TCP/IP as the standard protocol for inter-system communications over the ARPANET. The network was eventually split into two separate networks – the ARPANET continued to be used primarily for research purposes, while the MILNET became a military network.

In 1986, the National Science Foundation created the NSFNET, linking together the United States' supercomputing centers. Originally intended as a means for universities and other research institutes to access the ARPANET and exchange information, the NSFNET eventually replaced the ARPANET and became the backbone of today's Internet. Over 10,000 computer systems were connected to the Internet by 1989. Today the Internet's backbone is owned and operated by major Internet Service Providers (ISPs) such as GTE, MCI, Sprint, UUNet, and America Online. Connected to the backbone are many smaller networks which include university computing networks, government systems, and local ISPs.

Today’s Internet has become not only a major research network but also an enormous electronic medium that facilitates the commercial exchange of goods and services. Worldwide in its reach, the Internet has far exceeded its original designers' expectations and promises to become the world's major communications network.

 **STRUCTURE OF THE INTERNET**

The Internet is a loose amalgamation of computer networks run by many different organizations in over seventy countries. Most of the technological decisions are made by small committees of volunteers who set standards for interoperability.

The US portion of the Internet is best thought of as having three levels. At the bottom are local area networks (LANs); for example, campus networks. Usually the local networks are connected to a regional, or mid-level network. The mid-levels connect to one or more backbones. A backbone is an overarching network to which multiple regional networks connect, and which generally does not serve directly any local networks or end-users. The U.S. backbones connect to other backbone networks around the world. There are, however, numerous exceptions to this structure.

Most backbone and regional network traffic moves over leased phone lines. However, there is a fundamental distinction in how the lines are used by the Internet and the phone companies. The Internet provides connectionless packet-switched service whereas telephone service is circuit-switched. The difference may sound arcane, but it has vastly important implications for pricing and the efficient use of network resources.

Phone networks use circuit switching: an end-to-end circuit must be set up before the call can begin. A fixed share of network resources is reserved for the call, and no other call can use those resources until the original connection is closed. This means that a long silence between two teenagers uses the same resources as an active negotiation between two fast-talking lawyers. One advantage of circuit-switching is that it enables performance guarantees such as guaranteed maximum delay, which is essential for real-time applications like voice conversations.

The Internet uses “packet-switching” technology. The term “packets” refers to the fact that the data stream from your computer is broken up into packets of about 200 bytes (on average), which are then sent out onto the network. Each packet contains a “header” with information necessary for routing the packet from origination to destination. Thus each packet in a data stream is independent. The main advantage of packet-switching is that it permits “statistical multiplexing” on the communication lines. That is, the packets from many different sources can share a line, allowing for very efficient use of the fixed capacity.

**IP ADDRESSES**

Each computer on the Internet has a unique numerical address, called an Internet Protocol (IP) address, used to route packets to it across the Internet. Just as your postal address enables the postal system to send mail to your house from anywhere around the world, your computer's IP address gives the Internet routing protocols the unique information they need to route packets of information to your desktop from anywhere across the Internet. If a machine needs to contact another by a domain name, it first looks up the corresponding IP address with the domain name service.

The IP address is the geographical descriptor of the virtual world, and the addresses of both source and destination systems are stored in the header of every packet that flows across the Internet. You can find your IP address on a Windows computer by opening an MSDOS or Command window and typing one of "winipcfg" or "ipconfig". You can find your IP address on a Mac computer by checking your Network control panel. As described in the pages on confidentiality and privacy, Internet sites can and do track your IP address and other information. If you want to block or disguise your IP address, you can use an anonymizer.

An IP address is made up of four bytes of information (totaling 32 bits) expressed as four numbers between 0 and 255 shown separated by periods. For example, your computer's IP address might be 238.17.159.4, which is shown below in human-readable decimal form and in the binary form used on the Internet.

**SNEAKY WAYS TO GET AROUND THOSE INTERNET PRIVACY ISSUES**

Spam is a problem on the Internet, coming at us from just about every angle of the online space. Some spammers develop sophisticated, well-planned strategies, while others can be sloppy and still drive results. Either way, spam tactics come in a variety of shades, and it’s up to users to identify signals early on and avoid unsolicited content. Here’s a look at some spam tactics used in popular Internet spaces. Become familiar with these tactics to help identify them and avoid them whenever possible.

Spam on Social Media

A lot of the time, spam on social media is just bad social media marketing, or content marketing gone array. Being on either end (sending or receiving) of social media spam is not a good place to be. For receiving parties, it can be frustrating and even dangerous, depending on what the intention of the spammer is; and for senders, it’s extremely unprofessional and not a good way of building rapport with an audience.

The most dangerous spammers on social media are not simply interested in poorly marketing a product; they’re interested in releasing malware and ransomware, as well as persuading unsuspecting users to reveal personal information which can later result in identity theft.

To avoid social media scammers, it is recommended that you increase the security settings on your social media accounts. Moreover, you should be dubious of ‘liking’ or ‘sharing’ any posts that look suspicious, especially if they’re from people you don’t know or recognize. Check your applications in the settings menu of your accounts regularly. Delete, don’t just uninstall, applications that you don’t recognize. And finally, be cautious of connecting with people you don’t know online. A simple friend request can lead to a monsoon of spam and unwanted content. Make an effort to avoid these things by remaining vigilant while using social media.

Email Spam

This type of spam is often more sophisticated than what you might see on social media or in pop-up windows around the Web. That’s because email service providers like Google and Yahoo have gone to great lengths to improve the user experience by developing anti-spam filters and special algorithms to detect unwanted solicitations, which, of course, include email spam.

Spam is often referred to as ‘junk mail’. These communications are unwanted solicitations postured to sell something or incite further online action through the use of automated email correspondence. Most of the time, spam is harmless. However, spam is sometimes disguised to look like official communication between you and your financial institution, or a government agency.

In the cases above, the objective of the spammer is to get the user to click through and take further action. Just clicking a link can trigger a malware or ransomware. Other times, clicking through will take you to a landing page that looks strangely similar to your bank’s website or medical portal.

Usually, the user is prompted to type in personal information to continue.

Requests for your login and password, social security number, and phone number are popular ones from online identity thieves.

To avoid these sneaky tactics, look carefully at the email before clicking through. Do you recognize the sender? Does the subject line look suspicious?

Also, if you’re unsure whether a website is legitimate, always err on the side of caution. Look for security features like HTTPS extension at the beginning of the URL.

Do you see a small padlock or green bar over the URL? If these things are missing, the website is not operating with standard security features, and you should exit the site immediately.

Spam is all over the Internet, and if you’re not careful you can unintentionally become a victim of identity theft. Take steps to secure your computer and always practice vigilance when using email or social media to ensure your safety and to enjoy a more comfortable user experience online.

**PRIVACY WHILE BROWSING THE WEB**

Online activities often expose our sensitive information to the unwanted attention of many prying eyes. Every time that we are connected, our data can be collected with or without our authorization by many different parties. Internal software or computer vulnerabilities can also worsen the problem by compromising our anonymity.

When all this information is combined like a puzzle, our privacy could be violated, and our information accessed by unauthorized sources. However, online privacy violations are not committed only by criminals such as snoopers, hackers and cyberstalkers. Worldwide scandals such as Edward Snowden’s leaks only exposed the tip of the iceberg, as they revealed how national governments such as the American and British ones spied on millions of citizens.

Many new tools and software keep promising to ensure our security while browsing the internet, or at least, to protect our privacy by preserving our most sensitive information. The main question is, do they really work? And if they do, to what extent? Let’s have a look.

Enter your email address...

Anti-Virus and Firewall Suites

Firewalls and anti-viruses have been a staple in internet security for years. Technically a necessity to keep our data away from evildoers, they are apparently required only by those “unfortunate” enough to work and browse in a non-Mac environment. According to what most Mac experts and users like to boast, these tools seemingly filled the security gap left by the many Windows vulnerabilities. However, recent reports from Malwarebytes found that Mac malware increased by 230 percent during 2017, suggesting that these problems might endanger any and all operating systems.

There are many anti-virus programs available online, and not every one of them needs to be purchased. Although the idea of free and open-source software might be enticing, the recent security issues that hit even Avast, the most-installed free anti-virus in the world, taught many users that there’s no door that cannot be opened by a skilled hacker (or so it seems).

Paid anti-viruses also seemingly had their own issues with privacy leaks, though. In September 2017, the U.S. Secretary of Homeland Security Elaine Duke required all federal government agencies to stop using software developed by the Russian tech firm Kaspersky Lab. Due to heightening tension between the U.S. and Russia, concerns arose that Kaspersky may provide users' private information to the Russian government. Although Kaspersky obviously denied any wrongdoing, the haunting doubt struck the market and affected the opinion of many consumers.

Virtual Private Networks (VPNs)

With the increasingly widespread use of public connections and Wi-Fi hotspots, virtual private networks (VPNs) have become one of the most popular solutions to secure network access and all forms of online communication. Since the world of VPN services is split between free and paid services, the natural question is, once again, “is paying really necessary?” (Learn more about VPNs in Faceoff: Virtual Desktop Infrastructures Vs. Virtual Private Networks.)

For the most part, the biggest difference between paid and free services lies with many factors which are not related to security itself, such as data allowance and speed. However, some paid services also offer a 256-bit encryption working on much more secure protocols such as OpenVPN, rather than the standard PPTP. Yet, encryption only means that a VPN is harder to hack, but with enough computer resources applied to the decryption process, there’s no nut that can't be cracked.

An important point, though, is how user information is handled by VPN providers. If a log of user activity is kept, anonymity can be breached, for example, when a government authority requests these logs to be submitted during criminal investigations. Some smaller companies found a legal way to get around this limitation by not keeping any log, which cannot then be requested, although many usually just keep their logs for a shorter time period. A very small handful of them, however, simply do not have any log at all. Period.

Private/Incognito Mode

Many browsers offer a so-called “Incognito mode,” also known as InPrivate Browsing or Private window. Although this “privacy mode” is still worth mentioning for the sake of completeness, it has nothing to do with online security – even a little. Literally like treating a gaping gunshot wound with a Band-Aid, surfing in Incognito browsing mode simply keeps your browsing history and cache hidden from anyone who has access to your computer.

Cookies are not stored, text written into search bars is not saved in autofill fields, passwords are not saved, and the pages you visited are not recorded. That’s pretty much all it does. It can help you feel a little more anonymous when your wife, husband or kids access your computer, but it does not prevent any website or ISP from tracking your data.

**WEBSITE PRIVACY POLICY**

What is a website privacy policy?

A website privacy policy outlines your business practices in relation to the collection, storage and use of personal data gathered on your website. Examples of data include names, dates of birth, contact details or credit card details. It sets out the purpose of data collection on your website, the types of information collected and the scope and limitation of data processing on your website.

Why do you need a privacy policy?

The collection and use of personal data by online businesses in the UK must comply with the UK data protection laws and the GDPR. This policy is designed to allow the website operator to comply with the fair processing obligation and to obtain the user's consent to that processing as required by law.

Who is a Data Protection Officer (DPO)?

A Data Protection Officer assists your business with internal compliance and can inform or advise you of your data protection obligations, provide recommendations regarding any Data Protection Impact Assessments and act as a contact point for data subjects and the Information Commission Office (ICO).

What types of information will be collected from users?

It depends on the purpose for which the data is gathered. If you are selling and trading on your website, you may wish to collect your customers personal data such as names & credit card details. However, the data protection law defines personal data as broad as to include information about personal opinions and IP addresses.

What are cookies?

Cookies are small text files placed on a users computer, which are commonly used to collect personal data. Most website operators place cookies on the browser or hard drive of their users computer. Cookies can gather information about the users use of the website or enable the website to recognise the user as an existing customer when he returns to the website at a later date. The law protects users of your website and lets them opt out from the use of cookies on their website browser.

This document allows you to specify the types of cookies, their purpose and the method that will be used to gain consent of the user for the use of these cookies.

Do I need to display my personal details?

If you are a UK registered business you will need to disclose certain information about your company on your website or website privacy policy. You must display registered information such as:

Company name

Registered number

Place of registration

Registered office address

Contact details, including an email address

Details of how to contact the business

For sole traders and individuals, you must display the address of the principle place of business.

What's an Information Management Security System (IMSS)?

An IMSS is a set of principles and procedures for systematically managing an organisation's data. The goal of an IMSS is to minimise the risk for the business and ensure business continuity by pro-actively limiting the impact of a security breach. These practices relate to the protection of information, and are developed in accordance with the business position.

**Module II**

**\_\_\_\_\_\_\_\_\_\_\_\_INTERNET SERVICES \_\_\_\_\_\_\_\_**

**INTERNET PROTOCOL SUITE**

The Internet protocol suite is the conceptual model and set of communications protocols used on the Internet and similar computer networks. It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). It is occasionally known as the Department of Defense (DoD) model because the development of the networking method was funded by the United States Department of Defense through DARPA.

The Internet protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. This functionality is organized into four abstraction layers, which classify all related protocols according to the scope of networking involved.[1][2] From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment (link); the internet layer, providing internetworking between independent networks; the transport layer, handling host-to-host communication; and the application layer, providing process-to-process data exchange for applications.

Technical standards specifying the Internet protocol suite and many of its constituent protocols are maintained by the Internet Engineering Task Force (IETF). The Internet protocol suite predates the OSI model, a more comprehensive reference framework for general networking systems.

The Internet protocol suite resulted from research and development conducted by the Defense Advanced Research Projects Agency (DARPA) in the late 1960s.[3] After initiating the pioneering ARPANET in 1969, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation, in which the differences between local network protocols were hidden by using a common internetwork protocol, and, instead of the network being responsible for reliability, as in the ARPANET, this function was delegated to the hosts. Cerf credits Hubert Zimmermann and Louis Pouzin, designer of the CYCLADES network, with important influences on this design. The protocol was implemented as the Transmission Control Program, first published in 1974.[4]

Initially, the TCP managed both datagram transmissions and routing, but as the protocol grew, other researchers recommended a division of functionality into protocol layers. Advocates included Jonathan Postel of the University of Southern California's Information Sciences Institute, who edited the Request for Comments (RFCs), the technical and strategic document series that has both documented and catalyzed Internet development.[5] Postel stated, "We are screwing up in our design of Internet protocols by violating the principle of layering."[6] Encapsulation of different mechanisms was intended to create an environment where the upper layers could access only what was needed from the lower layers. A monolithic design would be inflexible and lead to scalability issues. The Transmission Control Program was split into two distinct protocols, the Transmission Control Protocol and the Internet Protocol.

**FILE TRANSFER PROTOCOL**

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.[2][3] Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as web page editors.

FTP may run in active or passive mode, which determines how the data connection is established.[6] In both cases, the client creates a TCP control connection from a random, usually an unprivileged, port N to the FTP server command port 21.

In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its port 20, the FTP server data port.

In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server,[6] which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.[7]

Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.[8]

The server responds over the control connection with three-digit status codes in ASCII with an optional text message. For example, "200" (or "200 OK") means that the last command was successful. The numbers represent the code for the response and the optional text represents a human-readable explanation or request (e.g. <Need account for storing file>).[1] An ongoing transfer of file data over the data connection can be aborted using an interrupt message sent over the control connection.

While transferring data over the network, four data representations can be used:[2][3][4]

ASCII mode: Used for text. Data is converted, if needed, from the sending host's character representation to "8-bit ASCII" before transmission, and (again, if necessary) to the receiving host's character representation. As a consequence, this mode is inappropriate for files that contain data other than plain text.

Image mode (commonly called Binary mode): The sending machine sends each file byte by byte, and the recipient stores the bytestream as it receives it. (Image mode support has been recommended for all implementations of FTP).

EBCDIC mode: Used for plain text between hosts using the EBCDIC character set.

Local mode: Allows two computers with identical setups to send data in a proprietary format without the need to convert it to ASCII.

For text files, different format control and record structure options are provided. These features were designed to facilitate files containing Telnet or ASA.

Data transfer can be done in any of three modes:[1][2]

Stream mode: Data is sent as a continuous stream, relieving FTP from doing any processing. Rather, all processing is left up to TCP. No End-of-file indicator is needed, unless the data is divided into records.

Block mode: FTP breaks the data into several blocks (block header, byte count, and data field) and then passes it on to TCP.[4]

Compressed mode: Data is compressed using a simple algorithm (usually run-length encoding).

Some FTP software also implements a DEFLATE-based compressed mode, sometimes called "Mode Z" after the command that enables it. This mode was described in an Internet Draft, but not standardized.[9]

**THREE WAYS TO MAKE SURE YOUR ONLINE CREDIT CARD TRANSACTION IS SAFE**

Your credit card isn't safe anywhere, especially the internet. When you're shopping online with your credit card, it's important to follow some guidelines to avoid credit card fraud and identity theft.

01 Only use your credit card on websites you trust.

When you shop with your credit card online, it's important that you only go to websites you trust. Avoid clicking on email links, particularly in unsolicited emails, because these links could take you to a fake website that's set up for the sole purpose of stealing your credit card information. Instead, go directly to the real website by typing the URL in your internet browser.

02 Don't make online credit card purchases from public places.

Public computers and networks are less secure so there's a greater chance that your credit card information can be stolen when you use it to make purchases on a public computer. These computers could have a keylogger software that will capture all your keystrokes, including your login information and credit card number.

You're not safe just because you're using your own computer on a public wifi. Hackers have access to the same wifi signal and can intercept information while it's being transmitted. That means no online ordering while you're using the wifi at your local coffee shop.

03 Protect your computer from viruses and hackers.

Make sure your computer is protected from hackers that could send your internet browser to a fake website by loading the most recent anti-virus and anti-spyware software onto your computer. Use only reputable anti-virus software, not anything you see in a pop-up advertisement or get as a link in an email.

04 Check with the Better Business Bureau.

If you're using your credit card online at a store you're not familiar with, check the Better Business Bureau or other consumer reports before entering your credit card information. Don't use your credit card at any website that has a poor customer service record with the Better Business Bureau.

**PUBLIC KEY CRYPTOGRAPHY**

Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

In a public key encryption system, any person can encrypt a message using the receiver's public key. That encrypted message can only be decrypted with the receiver's private key. To be practical, the generation of a public and private key -pair must be computationally economical. The strength of a public key cryptography system relies on the computational effort (work factor in cryptography) required to find the private key from its paired public key. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.[1]

Public key cryptography systems often rely on cryptographic algorithms based on mathematical problems that currently admit no efficient solution, particularly those inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. Public key algorithms, unlike symmetric key algorithms, do not require a secure channel for the initial exchange of one or more secret keys between the parties.[2]

Because of the computational complexity of asymmetric encryption, it is usually used only for small blocks of data, typically the transfer of a symmetric encryption key (e.g. a session key). This symmetric key is then used to encrypt the rest of the potentially long message sequence. The symmetric encryption/decryption is based on simpler algorithms and is much faster.[3]

In a public key signature system, a person can combine a message with a private key to create a short digital signature on the message. Anyone with the corresponding public key can combine a message, a putative digital signature on it, and the known public key to verify whether the signature was valid, i.e. made by the owner of the corresponding private key. Changing the message, even replacing a single letter, will cause verification to fail. In a secure signature system, it is computationally infeasible for anyone who does not know the private key to deduce it from the public key or any number of signatures, or to find a valid signature on any message for which a signature has not hitherto been seen. Thus the authenticity of a message can be demonstrated by the signature, provided the owner of the private key keeps the private key secret.[4][5]

Public key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA).

Public key cryptography finds application in, among others, the information technology security discipline, information security. Information security (IS) is concerned with all aspects of protecting electronic information assets against security threats.[6] Public key cryptography is used as a method of assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage.

**DECIPHERING INTERNET E-MAIL**

This guide is provided to learn how to read and understand an email header. To understand an email header, we need to analyze the life of the email. Most of the time, it appears that email is passed directly from the sender directly to the recipient. This isn't necessarily true: A typical email passes through at least four computers.

To begin you will need to find your full email header. You can find instructions at: How to View Email Headers.

VIEWING AN EMAIL HEADER

In this example, the "Sender" mt.kb.user@gmail.com wants to send an email to the "Receiver" user@example.com. The sender composes the email at gmail.com, and user@example.com receives it in the email client Apple Mail.

Here is the example header:

From: Media Temple user (mt.kb.user@gmail.com)

Subject: article: How to Trace a Email

Date: January 25, 2011 3:30:58 PM PDT

To: user@example.com

Return-Path: <mt.kb.user@gmail.com>

Envelope-To: user@example.com

Delivery-Date: Tue, 25 Jan 2011 15:31:01 -0700

Received: from po-out-1718.google.com ([72.14.252.155]:54907) by cl35.gs01.gridserver.com with esmtp (Exim 4.63) (envelope-from <mt.kb.user@gmail.com>) id 1KDoNH-0000f0-RL for user@example.com; Tue, 25 Jan 2011 15:31:01 -0700

Received: by po-out-1718.google.com with SMTP id y22so795146pof.4 for <user@example.com>; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)

Received: by 10.141.116.17 with SMTP id t17mr3929916rvm.251.1214951458741; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)

Received: by 10.140.188.3 with HTTP; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)

UNDERSTANDING THE EMAIL HEADER

CAUTION:

It is important to know that when reading an email header every line can be forged, so only the Received: lines that are created by your service or computer should be completely trusted.

From

This displays who the message is from, however, this can be easily forged and can be the least reliable.

Subject

This is what the sender placed as a topic of the email content.

Date

This shows the date and time the email message was composed.

To

This shows to whom the message was addressed, but may not contain the recipient's address.

Return-Path

The email address for return mail. This is the same as "Reply-To:".

Envelope-To

This header shows that this email was delivered to the mailbox of a subscriber whose email address is user@example.com.

Delivery Date

This shows the date and time at which the email was received by your (mt) service or email client.

Received

The received is the most important part of the email header and is usually the most reliable. They form a list of all the servers/computers through which the message traveled in order to reach you.

The received lines are best read from bottom to top. That is, the first "Received:" line is your own system or mail server. The last "Received:" line is where the mail originated. Each mail system has their own style of "Received:" line. A "Received:" line typically identifies the machine that received the mail and the machine from which the mail was received.

Dkim-Signature & Domainkey-Signature

These are related to domain keys which are currently not supported by (mt) Media Temple services. You can learn more about these by visiting: http://en.wikipedia.org/wiki/DomainKeys.

Message-id

A unique string assigned by the mail system when the message is first created. These can easily be forged.

Mime-Version

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email. Please see http://en.wikipedia.org/wiki/MIME for more details.

Content-Type

Generally, this will tell you the format of the message, such as html or plaintext.

X-Spam-Status

Displays a spam score created by your service or mail client.

X-Spam-Level

Displays a spam score usually created by your service or mail client.

Message Body

This is the actual content of the email itself, written by the sender.

FINDING THE ORIGINAL SENDER

The easiest way for finding the original sender is by looking for the X-Originating-IP header. This header is important since it tells you the IP address of the computer that had sent the email. If you cannot find the X-Originating-IP header, then you will have to sift through the Received headers to find the sender's IP address. In the example above, the originating IP Address is 10.140.188.3.

Once the email sender's IP address is found, you can search for it at http://www.arin.net/. You should now be given results letting you know to which ISP (Internet Service Provider) or webhost the IP address belongs. Now, if you are tracking a spam email, you can send a complaint to the owner of the originating IP address. Be sure to include all the headers of the email when filing a complaint.

**E-MAIL PROTOCOLS**

What is POP3 and which are the default POP3 ports

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

Port 110 - this is the default POP3 non-encrypted port

Port 995 - this is the port you need to use if you want to connect using POP3 securely

What is IMAP and which are the default IMAP ports

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

Port 143 - this is the default IMAP non-encrypted port

Port 993 - this is the port you need to use if you want to connect using IMAP securely

What is SMTP and which are the default SMTP ports

Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

By default, the SMTP protocol works on three ports:

Port 25 - this is the default SMTP non-encrypted port

Port 2525 - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP

Port 465 - this is the port used if you want to send messages using SMTP securely