Debit Card

A debit card (also known as a bank card or check card) is a plastic card that provides the cardholder electronic access to his or her bank account/s at a financial institution. Some cards have a stored value with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a designated account in favor of the payee's designated bank account. The card can be used as an alternative payment method to cash when making purchases. In some cases, the cards are designed exclusively for use on the Internet, and so there is no physical card.[1][2]

In many countries the use of debit cards has become so widespread that their volume of use has overtaken or entirely replaced the check and, in some instances, cash transactions. Like credit cards, debit cards are used widely for telephone and Internet purchases.

However, unlike credit cards, the funds paid using a debit card are transferred immediately from the bearer's bank account, instead of having the bearer pay back the money at a later date.

Debit cards usually also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash and as a check guarantee card. Merchants may also offer cashback facilities to customers, where a customer can withdraw cash along with their purchase.

There are currently three ways that debit card transactions are processed: online debit (also known as PIN debit), offline debit (also known as signature debit) and the Electronic Purse Card System.[3] One physical card can include the functions of an online debit card, an offline debit card and an electronic purse card.

Advantages of debit cards

A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can more easily obtain a debit card, allowing him/her to make plastic transactions. For example, legislation often prevents minors from taking out debt, which includes the use of a credit card, but not online debit card transactions.

For most transactions, a check card can be used to avoid check writing altogether. Check cards debit funds from the user's account on the spot, thereby finalizing the transaction at the time of purchase, and bypassing the requirement to pay a credit card bill at a later date, or to write an insecure check containing the account holder's personal information.

Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks, thereby making transactions quicker and less intrusive. Unlike personal checks, merchants generally do not believe that a payment via a debit card may be later dishonored.

Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge, other than a foreign ATM fee.

Disadvantages of debit cards

Use of a debit card is not usually limited to the existing funds in the account to which it is linked, most banks allow a certain threshold over the available bank balance which can cause overdraft fees if the user's transaction does not reflect available balance. This disadvantage has lessened in the United States with the requirement that an issuer obtain opt-in permission in advance to allow an overdraft on a debit card. Lacking this opt-in, overdrafts are not permitted for electronic transactions.

Many banks are now charging over-limit fees or non-sufficient funds fees based upon pre-authorizations, and even attempted but refused transactions by the merchant (some of which may be unknown until later discovery by account holder).

Many merchants mistakenly believe that amounts owed can be "taken" from a customer's account after a debit card (or number) has been presented, without agreement as to date, payee name, amount and currency, thus causing penalty fees for overdrafts, over-the-limit, amounts not available causing further rejections or overdrafts, and rejected transactions by some banks.

In some countries debit cards offer lower levels of security protection than credit cards.[8] Theft of the users PIN using skimming devices can be accomplished much easier with a PIN input than with a signature-based credit transaction. However, theft of users' PIN codes using skimming devices can be equally easily accomplished with a debit transaction PIN input, as with a credit transaction PIN input, and theft using a signature-based credit transaction is equally easy as theft using a signature-based debit transaction.

In many places, laws protect the consumer from fraud much less than with a credit card. While the holder of a credit card is legally responsible for only a minimal amount of a fraudulent transaction made with a credit card, which is often waived by the bank, the consumer may be held liable for hundreds of dollars, or even the entire value of fraudulent debit transactions. The consumer also has a shorter time (usually just two days) to report such fraud to the bank in order to be eligible for such a waiver with a debit card,[8] whereas with a credit card, this time may be up to 60 days. A thief who obtains or clones a debit card along with its PIN may be able to clean out the consumer's bank account, and the consumer will have no recourse.

Security in E Commerce

There are different types of security measures that you can take to protect your virtual storefront. This is so important, as the customer's information has to be shielded from everybody else, must not be open to alteration or tampering, whilst going through the process of authentication and receipt. Make sure that you digitally reproduce information that will tell your clients about the type of security used. It's like hanging a certificate behind the counter in a physical store.

Digital signatures are a way of authenticating the sender and receiver of information. When making a transaction you can ask for a password as a digital signature. Have you seen those boxes with jumbled letters and numbers they ask you to copy in the box? That can be used to verify who you are.

You put a digital signature on your storefront, didn't you? This helps customers to be confident that you are who you claim to be. This is a line of defence against being "conned" by would-be impostors, who just want access to your money.

The acronym SSL means "secure socket layer." You may have seen those initials or seen the closed or open lock on a website page. You can click on the lock to view certificates and find out if the website is actually encrypted. Behind the scenes, information is encrypted using a public key and a private key. Technically speaking, the public element is used to encrypt and a private one used to decrypt. From the customer to the server, to your server to the payment gateway, and the credit card issuer, several layers of security come into play.

Firewalls are used specifically to block unwanted intrusions. You almost certainly have one on your personal computer at home. Make sure that you have a firewall on your website, so that others cannot access any customer data that may be stored on your server. Don't take the risk, as a few "on point" virtual assistants can make all the difference in your long-term goals.

From both the point of view of the customer and your own business interests, pay particular attention to security. You have the technology at your disposal to keep your customer data safe from the ever-growing number of online criminals.

E Commerce Payment System

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

There are numerous different payments systems available for online merchants. These include the traditional credit, debit and charge card but also new technologies such as digital wallets, e-cash, mobile payment and e-checks. Another form of payment system is allowing a 3rd party to complete the online transaction for you. These companies are called Payment Service Providers (PSP).

Over the years, credit cards have become one of the most common forms of payment for e-commerce transactions. In North America almost 90% of online B2C transactions were made with this payment type [1]. Turban et al. goes on to explain that it would be difficult for an online retailer to operate without supporting credit and debit cards due to their widespread use. Increased security measures such as the use of the card verification number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank [2]. Also online merchants have to comply with stringent rules stipulated by the credit and debit card issuers (Visa and MasterCard)[3] this means that merchants must have security protocol and procedures in place to ensure transactions are more secure. This can also include having a certificate from an authorized certification authority (CA) who provides PKI infrastructure for securing credit and debit card transactions.

Despite this widespread use in North America, there are still a large number of countries such as China, India and Pakistan that have some problems to overcome in regard to credit card security. In the meantime, the use of smartcards has become extremely popular. A Smartcard is similar to a credit card; however it contains an embedded 8-bit microprocessor and uses electronic cash which transfers from the consumers' card to the sellers' device. A popular smartcard initiative is the VISA Smartcard. Using the VISA Smartcard you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the internet.

There are companies that enable financial transactions to transpire over the internet, such as PayPal. Many of the mediaries permit consumers to establish an account quickly, and to transfer funds into their on-line accounts from a traditional bank account (typically via ACH transactions), and vice versa, after verification of the consumer's identity and authority to access such bank accounts. Also, the larger mediaries further allow transactions to and from credit card accounts, although such credit card transactions are usually assessed a fee (either to the recipient or the sender) to recoup the transaction fees charged to the mediary.

Internet Explorer

Windows Internet Explorer (formerly Microsoft Internet Explorer, commonly abbreviated IE or MSIE) is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995. It was first released as part of the add-on package Plus! for Windows 95 that year. Later versions were available as free downloads, or in service packs, and included in the OEM service releases of Windows 95 and later versions of Windows.

Internet Explorer has been the most widely used web browser since 1999, attaining a peak of about 95% usage share during 2002 and 2003 with Internet Explorer 5 and Internet Explorer 6.[citation needed] Since its peak of popularity, its usage share has been declining in the face of renewed competition from other web browsers, and is currently 40.9% as of June 2011. It had been slightly higher, 43.55% as of February 2011, just prior to the release of the current version. Microsoft spent over $100 million USD per year on Internet Explorer in the late 1990s,[1] with over 1000 people working on it by 1999.

Since its first release, Microsoft has added features and technologies such as basic table display (in version 1.5); XMLHttpRequest (in version 5), which aids creation of dynamic web pages; and Internationalized Domain Names (in version 7), which allow Web sites to have native-language addresses with non-Latin characters. The browser has also received scrutiny throughout its development for use of third-party technology (such as the source code of Spyglass Mosaic, used without royalty in early versions) and security and privacy vulnerabilities, and both the United States and the European Union have alleged that integration of Internet Explorer with Windows has been to the detriment of other browsers.

The latest stable release is Internet Explorer 9, which is available as a free update for Windows 7, Windows Vista SP2, Windows Server 2008, and Windows Server 2008 R2. Internet Explorer was to be omitted from Windows 7 and Windows Server 2008 R2 in Europe, but Microsoft ultimately included it, with a browser option screen allowing users to select any of several web browsers (including Internet Explorer).

Versions of Internet Explorer for other operating systems have also been produced, including an embedded OEM version called Pocket Internet Explorer, later rebranded Internet Explorer Mobile, which is currently based on Internet Explorer 7 and made for Windows Phone 7, Windows CE, and previously Windows Mobile. It remains in development alongside the more advanced desktop versions. Internet Explorer for Mac and Internet Explorer for UNIX (Solaris and HP-UX) have been discontinued.

Internet Security

Internet security is a branch of computer security[1] specifically related to the Internet. Its objective is to establish rules and measures to use against attacks over the Internet.[2] The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing.[3] Different methods have been used to protect the transfer of data, including encryption.

Network layer security

TCP/IP can be made secure with the help of cryptographic methods and protocols that have been developed for securing communications on the Internet. These protocols include SSL and TLS for web traffic, PGP for email, and IPsec for the network layer security.

IPsec Protocol

This protocol is designed to protect communication in a secure manner using TCP/IP. It is a set of security extensions developed by IETF, and it provides security and authentication at the IP layer by using cryptography. To protect the content, the data is transformed using encryption techniques. There are two main types of transformation that form the basis of IPsec: the Authentication Header (AH) and Encapsulating Security Payload (ESP). These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

The basic components of the IPsec security architecture are described in terms of the following functionalities:

Security protocols for AH and ESP

Security association for policy management and traffic processing

Manual and automatic key management for the internet key exchange (IKE)

Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

Netscape Navigator

Netscape Navigator was a proprietary web browser that was popular in the 1990s. It was the flagship product of the Netscape Communications Corporation and the dominant web browser in terms of usage share, although by 2002 its usage had almost disappeared. This was primarily due to the increased usage of Microsoft's Internet Explorer web browser software, and partly because the Netscape Corporation (later purchased by AOL) did not sustain Netscape Navigator's technical innovation after the late 1990s.

The business demise of Netscape was a central premise of Microsoft's antitrust trial, wherein the Court ruled that Microsoft Corporation's bundling of Internet Explorer with the Windows operating system was a monopolistic and illegal business practice. The decision came too late for Netscape however, as Internet Explorer had by then become the dominant web browser in Windows.

The Netscape Navigator web browser was succeeded by Netscape Communicator. Netscape Communicator's 4.x source code was the base for the Netscape-developed Mozilla Application Suite, which was later renamed SeaMonkey.[2] Netscape's Mozilla Suite also served as the base for a browser-only spinoff called Mozilla Firefox and Netscape versions 6 through 9.

AOL formally stopped development of Netscape Navigator on December 28, 2007, but continued supporting the web browser with security updates until March 1, 2008, when AOL canceled technical support. AOL allows downloading of archived versions of the Netscape Navigator web browser family. Moreover, AOL maintains the Netscape website as an Internet portal.

Netscape Navigator was based on the Mosaic web browser, which was co-written by Marc Andreessen, a part-time employee of the National Center for Supercomputing Applications and a student at the University of Illinois. After Andreessen graduated in 1993, he moved to California and there met Jim Clark, the recently-departed founder of Silicon Graphics. Clark believed that the Mosaic browser had great commercial possibilities and provided the seed money. Soon Mosaic Communications Corporation was in business in Mountain View, California, with Andreessen as a vice-president. Since the University of Illinois was unhappy with the company's use of the Mosaic name, the company changed its name to Netscape Communications (thought up by sales representative Greg Sands) and named its flagship web browser Netscape Navigator.

Online banking

Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.

Online banking solutions have many features and md capabilities in common, but traditionally also have some that are application specific.

The common features fall broadly into several categories

- Transactional (e.g., performing a financial transaction such as an account to account transfer, paying a bill, wire transfer, apply for a loan, new account, etc.)
    - Payments to third parties, including bill payments and telegraphic/wire transfers
    - Funds transfers between a customer's own transactional account and savings accounts
    - Investment purchase or sale
    - Loan applications and transactions, such as repayments of enrollments

- Non-transactional (e.g., online statements, cheque links, cobrowsing, chat)
    - Viewing recent transactions
    - Downloading bank statements, for example in PDF format
    - Viewing images of paid cheques
- Financial Institution Administration
- Management of multiple users having varying levels of authority
- Transaction approval process

Features commonly unique to Internet banking include

- Personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter. The most secure way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (two-factor authentication or 2FA). Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.

What is Online Retailing?

Online retailing (also known as B2C or business-to-consumer e-commerce) is basically a Web-enabled interface between your company and your target consumer for selling products and services on the Web with the facility of online payment.

What exactly can retailing do for you?

To compete in today's high-pressure business scenario, sellers are looking at the internet as a very effective alternative sales channel, which gives them direct access to target customers.

Here are some of the advantages it can give you:

- Requires lower investment (when compared to setting up a conventional, "brick-and-mortar" store)
- Extends your reach to new customers and new markets, and builds an extensive customer base
- Quicker Return on investment (RDI) than conventional, off-line selling
- Reduces customer acquisition costs by up to 70%
- Reduces transaction costs
- Reduces advertising and promotional costs
- Faster inventory turnover
- Improves your understanding of your customers on a 1-to-1 basis
- Helps serve your customer better by giving her greater choice and greater convenience of shopping
- Increases brand value and brand recall
- Eliminates geographical boundaries for your business, and can establish a global market for your product or service

Online retailing can be extremely useful to consumer product and service enterprise especially in the area of:

Apparel, Arts and Handicrafts, Books, Car rentals, Computers and Electronics, Cosmetics,

Financial Services, Gifts and Novelties, Groceries, Music, Software, Stationary, Sweets and Confectionery, Tours and Travels, toys, services of all types.

URL Types

This page defines and discusses varieties of URLs that will be encountered when working with vendor URLs. Each URL is a combination of these types. To illustrate this, some of the same URLs are used in multiple examples in the charts below.

Starting Point URLs

The goal in understanding vendor URLs is to determine the **starting point URL**. A starting point URL is a persistent, durable URL that connects a browser to a resource. This is the URL utilized in your OPAC, Web site, database, etc. to provide access to a resource. Ultimately, our goal is to determine starting point URLs.

The concept of the starting point URL is important for two reasons:

1. Many vendor URLs become transformed by programming scripts when they are selected, so that the destination URL is different from the starting point URL. In these cases, the destination URL is not persistent. It cannot be copied and pasted into your application to be used again, because it will fail.
2. Many vendors sites feature title lists that use URLs that are not structured to be persistent if used by their customers. If you use the URLs featured on these lists, your connections may fail.

The URLs described below are four different types of starting point URLs.

Static URL

Definition: A URL that connects to a desination without calling a script.

Example: http://muse.jhu.edu/journals/american_literature/

Discussion A static URL is a persistent, durable URL. No programming scripts are generated when a static URL is selected. Therefore the destination URL is identical to the starting point URL. A static URL is always a starting point URL.

Dynamic URL

Definition: A URL that processes a script to connect to a destination.

Example: http://www.springerlink.com/link.asp?id=100408

Discussion: Dynamic URLs are becoming increasingly common with vendors and should be analyzed carefully. Most become transformed at the destination.

For example, this URL, **http://firstsearch.oclc.org/dbname=WorldCat;done=referer;FSIP** becomes transformed to this:

http://firstsearch.oclc.org/WebZ/FSPrefs?entityjsdetect=:javascript=true:screensize=large:sessionid=fsapp3-36672-f5pysd37-7ipve9:entitypagenum=1:0

In this case, the destination URL is not persistent and therefore should not be used as a starting point URL.

Directory URL

Definition: A URL without a filename that points to a directory's default file.

Example: http://muse.jhu.edu/journals/american_literature/

Discussion:A directory URL may be either static or dynamic. A dynamic directory URL calls a script from a file given the Web server's default file name, e.g., default.asp. The script may be a simple redirect or something more complex.

VSAT

Satellite as a back up option

Satellite can act as an excellent back up option in places where the quality of terrestrial access is unreliable and/or poor. Satellite back up ensures that businesses and end users are connected to the Internet when the primary terrestrial access is unavailable for short periods of time.

Advantages of Satellite Internet

Global Coverage

This is the most significant advantage of using satellite links - coverage at any location on Earth. A single satellite in the geostationary orbit can cover distances as large as whole oceans or continents.

This wide area coverage makes high-speed Internet access from remote locations quick and easy. It is also possible to connect many remote locations spread across large distances through a secure private link.

Due to the curvature of the Earth, uneven terrain, oceans and many natural and man-made obstacles, it is difficult to set up a direct communication path over long distances. For businesses like off-shore oil exploration, it is nearly impossible to directly communicate with headquarters - hundreds of miles away. For such requirements, satellite is the most effective option. For satellite connectivity to be established, you only need a power supply and a clear view of the satellite orbiting at 23,000 miles in the geostationary orbit.

Take a look at the VSAT Systems Coverage Map to understand how we provide coverage across North America, Central America and the Caribbean.

High speed access

The first thing you would notice about satellite Internet is Speed. Most satellite Internet providers can provide multi megabit speeds which can be sometimes faster than terrestrial options. If the options available are limited, such as dial-up or unreliable/slow DSL, satellite is the clear winner.

VSAT Systems can provide end users with speeds as high as 2 Mbps upload and 4Mbps download with CIRs for guaranteed speeds.

Cost effective

It costs anywhere between $10,000- $100,000 to lay a mile of fiber in an unserved location. In addition to the high investment, it may take several months to complete the fiber deployment and

make it available to individual locations. If you do not have access to reliable terrestrial connectivity, satellite is the most cost-effective means of high-speed Internet access.

Location independent - mobile solutions

Having a broadband connection at any location is great, the advantage of taking it anywhere is even better.

Internet via satellite is possible through fixed and mobile equipment. The end user location is connected to the Internet as long as the VSAT dish has a clear line of sight (i.e. a clear view of the southern sky).

Bandwidth availability

The geo-stationary orbit has about 180 'parking spots' for satellites. Of these, many satellites have fixed positions over large oceans. These satellites are great for watching the weather, but are not useful for providing data communications services. For coverage over North America, there are only a few satellites that can do it. Of these few, fewer are available for Tier 1 operators. Some are exclusively owned by governments. Some are used for broadcast and telecommunications.

Even with the fact that there are limited 'parking spots' for satellites in the geo-stationary orbit and limited bandwidth on these satellites, operators such as Intelsat and Telesat have the capacity to provide gigabit speeds over entire continents. This bandwidth is less than what terrestrial options might have to offer. However, this bandwidth is available throughout the footprint bringing high-speed access at any location.

Reliability

As the satellite network consists of only a satellite, teleport, NOC and VSAT terminal, the number of opportunities for network outages are significantly reduced. Compared to terrestrial networks, there is much less opportunity for network outages. With terrestrial services (cable or DSL), network outages can occur at any point along the infrastructure.

A complete satellite network can work independently of terrestrial infrastructure and maintain connectivity as long as the equipment is powered.

Instant installation and deployment

The satellites antennas can be instantly deployed and installed within a matter of a few hours. For mobile and transportable solutions, you can set-up and connect to the Internet in less than 10 minutes.

WEB BROWSER

- Refresh button is used to *go back and forward* while browsing. If you are in a home page of some site, then you go to contact page – ***Back button*** would *bring you back to the home page*, if then you would click ***forward button*** it would bring you *again to the contact page*. A small arrow next to navigation buttons brings up a quick list of all back/forward web pages available.

- **Refresh**

- **button**

Refresh buttons is used to force web browser to reload webpage. Most major web browsers use caching mechanism (store local copies of visited pages to speed up performance) that sometimes *prevents seeing the most updated information*; *by clicking refresh, latest version of the page is forcefully reloaded.*

- **Stop**

- **button**

Cancels web browser's communication with a server and stops page loading. *Very useful to stop malicious sites from loading if accidentally entered.*

- **Home**

- **button**

Loads predefined home page. You can *select any page as browser's home* by clicking on tools menu and selecting options.

- **Web browser's address**

- **bar**

Address bar is used to *enter website and page names*. Address bar works as a dropdown menu showing all previously visited sites. At the end of address bar you will find *go button*, that is not very useful as by simply clicking enter *(after typing or selecting a domain name)* you will be directed to the site.

- **Integrated**

- **search**

Integrated search engine tool is relatively *new feature in web browsers*. It allows selecting your *favorite search engine* and doing a quick search by typing in a search term.

- **Tabbed**

- **browsing**

Browser tabs allow opening many websites on a single web browser's window - very helpful when reading several websites at the same time. I.e. if you want to open several links from a website without losing it, you can right click on each link you want to see, and select open in a new tab option.

- **Bookmark**

buttons

Custom user defined buttons that redirect to chosen websites - Very useful to configure web mail and other often visited sites. Check Mozilla Firefox browser for live bookmarking.

WEBSITE Maintaiannance

A web content management system (WCMS)[1] is a software system that provides website authoring, collaboration, and administration tools designed to allow users with little knowledge of web programming languages or markup languages to create and manage website content with relative ease. A robust WCMS provides the foundation for collaboration, offering users the ability to manage documents and output for multiple author editing and participation.

Most systems use a database to store page content, metadata, and other information assets that might be needed by the system.

A presentation layer displays the content to website visitors based on a set of templates. The templates are sometimes XSLT files.[2]

Most systems use server side caching to improve performance. This works best when the WCMS is not changed often but visits happen regularly.

Administration is typically done through browser-based interfaces, but some systems require the use of a fat client.

A WCMS allows non-technical users to make changes to a website with little training. A WCMS typically requires a systems administrator and/or a web developer to set up and add features, but it is primarily a website maintenance tool for non-technical staff.

A web content management system is used to control a dynamic collection of Web material, including HTML documents, images, and other forms of media.[3] A CMS facilitates document control, auditing, editing, and timeline management. A WCMS typically has the following features:[4][5]

Automated templates

Create standard output templates (usually HTML and XML) that can be automatically applied to new and existing content, allowing the appearance of all content to be changed from one central place.

Access Control

Some WCMS systems support user Groups. User Groups allow you to control how registered users interact with the site. A page on the site can be restricted to one or more groups. This means if an Anonymous User (someone not logged on) or a Logged on User who is not a member of the Group a page is restricted to, the user will be denied access to the page.

Scalable expansion

Available in most modern WCMSs is the ability to expand a single implementation (one installation on one server) across multiple domains, depending on the server's settings. WCMS sites may be able to create microsites/web portals within a main site as well.

Easily editable content

Once content is separated from the visual presentation of a site, it usually becomes much easier and quicker to edit and manipulate. Most WCMS software includes WYSIWYG editing tools allowing non-technical individuals to create and edit content.

Scalable feature sets

Most WCMS software includes plug-ins or modules that can be easily installed to extend an existing site's functionality.

Website Hosting

A **web hosting service** is a type of Internet hosting service that allows individuals and organizations to make their own website accessible via the World Wide Web. Web hosts are companies that provide space on a server they own or lease for use by their clients as well as providing Internet connectivity, typically in a data center. Web hosts can also provide data center space and connectivity to the Internet for servers they do not own to be located in their data center, called colocation or Housing as it is commonly called in Latin America or France.

The scope of web hosting services varies greatly. The most basic is web page and small-scale file hosting, where files can be uploaded via File Transfer Protocol (FTP) or a Web interface. The files are usually delivered to the Web "as is" or with little processing. Many Internet service providers (ISPs) offer this service free to their subscribers. People can also obtain Web page hosting from other, alternative service providers. Personal web site hosting is typically free, advertisement-sponsored, or inexpensive. Business web site hosting often has a higher expense.

Single page hosting is generally sufficient only for personal web pages. A complex site calls for a more comprehensive package that provides database support and application development platforms (e.g. PHP, Java, Ruby on Rails, ColdFusion, and ASP.NET). These facilities allow the customers to write or install scripts for applications like forums and content management. For e-commerce, SSL is also highly recommended.

The host may also provide an interface or control panel for managing the Web server and installing scripts as well as other modules and service applications like e-mail. Some hosts specialize in certain software or services (e.g. e-commerce). They are commonly used by larger companies to outsource network infrastructure to a hosting company.

The availability of a website is measured by the percentage of a year in which the website is publically accessible and reachable via the internet. This is different than measuring the uptime

of a system, as uptime refers to the system itself being online, however does not take into account being able to reach it – as in the event of a network outage.

Search Engine

A web search engine is designed to search for information on the World Wide Web and FTP servers. The search results are generally presented in a list of results often referred to as SERPS, or "search engine results pages". The information may consist of web pages, images, information and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories, which are maintained only by human editors, search engines also maintain real-time information by running an algorithm on a web crawler.

A search engine operates in the following order:

1. Web crawling
2. Indexing
3. Searching.

Web search engines work by storing information about many web pages, which they retrieve from the html itself. These pages are retrieved by a Web crawler (sometimes also known as a spider) — an automated Web browser which follows every link on the site. Exclusions can be made by the use of robots.txt. The contents of each page are then analyzed to determine how it should be indexed (for example, words are extracted from the titles, headings, or special fields called meta tags). Data about web pages are stored in an index database for use in later queries. A query can be a single word. The purpose of an index is to allow information to be found as quickly as possible. Some search engines, such as Google, store all or part of the source page (referred to as a cache) as well as information about the web pages, whereas others, such as AltaVista, store every word of every page they find. This cached page always holds the actual search text since it is the one that was actually indexed, so it can be very useful when the content of the current page has been updated and the search terms are no longer in it. This problem might be considered to be a mild form of linkrot, and Google's handling of it increases usability by satisfying user expectations that the search terms will be on the returned webpage. This satisfies the principle of least astonishment since the user normally expects the search terms to be on the returned pages. Increased search relevance makes these cached pages very useful, even beyond the fact that they may contain data that may no longer be available elsewhere.

When a user enters a query into a search engine (typically by using key words), the engine examines its index and provides a listing of best-matching web pages according to its criteria, usually with a short summary containing the document's title and sometimes parts of the text. The index is built from the information stored with the data and the method by which the information is indexed. Unfortunately, there are currently no known public search engines that

allow documents to be searched by date. Most search engines support the use of the boolean operators AND, OR and NOT to further specify the search query. Boolean operators are for literal searches that allow the user to refine and extend the terms of the search. The engine looks for the words or phrases exactly as entered. Some search engines provide an advanced feature called proximity search which allows users to define the distance between keywords. There is also concept-based searching where the research involves using statistical analysis on pages containing the words or phrases you search for. As well, natural language queries allow the user to type a question in the same form one would ask it to a human. A site like this would be ask.com.

WEB SERVER

Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet.[1]

The most common use of web servers is to host web sites but there are other uses such as data storage or running enterprise applications. The primary function of a web server is to deliver web pages on the request to clients. This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets and scripts.

A client, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if unable to do so. The resource is typically a real file on the server's secondary memory, but this is not necessarily the case and depends on how the web server is implemented.

While the primary function is to serve content, a full implementation of HTTP also includes ways of receiving content from clients. This feature is used for submitting web forms, including uploading of files.

Many generic web servers also support server-side scripting, e.g., Active Server Pages (ASP) and PHP. This means that the behaviour of the web server can be scripted in separate files, while the actual server software remains unchanged. Usually, this function is used to create HTML documents "on-the-fly" as opposed to returning fixed documents. This is referred to as dynamic and static content respectively. The former is primarily used for retrieving and/or modifying information from databases. The latter is, however, typically much faster and more easily cached.

Web servers are not always used for serving the world wide web. They can also be found embedded in devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring and/or administrating the device in question. This usually means that no additional software has to be installed on the

client computer, since only a web browser is required (which now is included with most operating systems).

Common features

- **Virtual hosting** to serve many Web sites using one IP address
- **Large file support** to be able to serve files whose size is greater than 2 GB on 32 bit OS
- **Bandwidth throttling** to limit the speed of responses in order to not saturate the network and to be able to serve more clients
- **Server-side scripting** to generate dynamic Web pages, still keeping web server and website implementations separate from each other

WEB Threat

A web threat is any threat that uses the internet to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.

Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.

It is a type of threat related to information technology (IT). The IT risk, i.e. risk affecting has gained and increasing impact on society due to the spread of IT processes.

Web threats can be divided into two primary categories, based on delivery method – push and pull.[4] Push-based threats use spam, phishing, or other fraudulent means to lure a user to a malicious (often spoofed) website which then collects information and/or injects malware. Push attacks use phishing, DNS poisoning (or pharming), and other means to appear to originate from a trusted source.

Precisely-targeted push-based web threats are often referred to as spear phishing to reflect the focus of their data gathering attack. Spear phishing typically targets specific individuals and groups for financial gain. In other push-based web threats, malware authors use social engineering such as enticing subject lines that reference holidays, popular personalities, sports,

pornography, world events and other hot topics to persuade recipients to open the email and follow links to malicious websites or open attachments with malware that accesses the Web.

Pull-based web threats are often referred to as "drive-by" threats, since they can affect any website visitor. Cybercriminals infect legitimate websites, which unknowingly transmit malware to visitors or alter search results to take users to malicious websites. Upon loading the page, the user's browser passively runs a malware downloader in a hidden HTML frame (IFRAME) without any user interaction.

WEBSITE Plaining

Most people understand the need for a website plan but don't know where to begin. These free tutorials will teach you everything you need to know to prepare a website plan that you can give to any developer. They will love you for it and your project is much more likely to run smoothly.

Each of the free Website Planning tutorials is concise so you can learn quickly. You can then get down to work and plan a site in as little as two hours. Topics covered include:

- What is a web host, what is a domain name and what does a website cost
- Understanding how search engines work and choosing an appropriate keyword
- Website goals – 18 examples and how to measure the results
- Competitor research, brainstorming and developing a site map
- Understanding the various elements on a web page
- How to write your website text

A **website**, also written as **Web site**,[1] **web site**, or simply **site**,[2] is a collection of related web pages containing images, videos or other digital assets. A website is hosted on at least one web server, accessible via a network such as the Internet or a private local area network through an Internet address known as a Uniform Resource Locator. All publicly accessible websites collectively constitute the World Wide Web.

A web page is a document, typically written in plain text interspersed with formatting instructions of Hypertext Markup Language (HTML, XHTML). A web page may incorporate elements from other websites with suitable markup anchors.

Web pages are accessed and transported with the Hypertext Transfer Protocol (HTTP), which may optionally employ encryption (HTTP Secure, HTTPS) to provide security and privacy for the user of the web page content. The user's application, often a web browser, renders the page content according to its HTML markup instructions onto a display terminal.

The pages of a website can usually be accessed from a simple Uniform Resource Locator (URL) called the homepage. The URLs of the pages organize them into a hierarchy, although hyperlinking between them conveys the reader's perceived site structure and guides the reader's navigation of the site.

Some websites require a subscription to access some or all of their content. Examples of subscription websites include many business sites, parts of news websites, academic journal websites, gaming websites, file-sharing websites, message boards, web-based email, social networking websites, websites providing real-time stock market data, and websites providing various other services (e.g., websites offering storing and/or sharing of images, files and so forth).

WEBSITE DESIGN

Web design is the process of planning and creating a website. Text, images, digital media and interactive elements are shaped by the web designer to produce the page seen on the web browser.[1] Web designers utilize markup language, most notably HTML for structure and CSS for presentation to develop pages that can be read by web browsers.

As a whole, the process of web design includes conceptualization, planning, producing, post-production, research, advertising as well as media control that is applied to the pages within the site by the designer or group of designers with a specific purpose. The site itself can be divided into its main page, also known as the home page, which cites the main objective as well as highlights of the site's daily updates; which also contains hyperlinks that functions to direct viewers to a designated page within the site's domain.

nitial website designs normally need small tweaks and changes after they go live, but major updates and re-designs may be undertaken periodically.

Changes to websites almost always provoke a backlash from its regular users.[6] The reason for this is primarily that change is disruptive to the user: for example, the link that the user previously learned was always in the lower left corner is now "missing", and the user must search the page to discover its new location. The user is disoriented, frustrated, slowed down, and needs time to learn and adapt to the new arrangement. On websites with users who spend significant amounts of time each day using, like Facebook or Wikipedia, users normally respond to even moderate changes with noisy protests and empty threats to leave the website.[6]

Within a few weeks or months, however, most users have adapted to the changes and no longer object to them.[6] For example, the signature feature of Facebook, a news feed, drew millions of complaints when it first appeared, but users now say that it is an important and highly desirable feature.[6]

Major websites may try to minimize this with phased rollouts of changes, testing the new design with a small number of randomly selected users, describing the importance of the upcoming changes in advance, and offering users the option of keeping the old design until they have acclimated to the new one. However, the primary cure for complaints is simply to wait.[6]

X.400

X.400 is a suite of ITU-T Recommendations that define standards for Data Communication Networks for Message Handling Systems (MHS) — more commonly known as "email".

At one time X.400 was expected to be the predominant form of email, but this has role has been taken by the SMTP-based Internet e-mail. Despite this, it has been widely used within organizations, was a core part of Microsoft Exchange Server until 2006, and variants continue to be important in military and aviation contexts.

An X.400 address consists of several elements, including:

- C (Country name)
- ADMD (Administration Management Domain), usually a public mail service provider
- PRMD (Private Management Domain)
- O (Organization name)
- OU (Organizational Unit Names)
- G (Given name)
- I (Initials)
- S (Surname)

The first X.400 Recommendations were published in 1984 (*Red Book*), and a substantially revised version was published in 1988 (*Blue Book*). New features were added in 1992 (*White Book*) and subsequent updates. Although X.400 was originally designed to run over the OSI Transport service, an adaptation to allow operation over TCP/IP, RFC 1006, has become the most popular way to run X.400.

Developed in cooperation with the ISO, the X.400-series recommendations specify OSI standard protocols for exchanging and addressing electronic messages. The companion F.400-series of recommendations define Message Handling Services built on Message Handling Systems (MHS), as well as access to and from the MHS for public services. In the late 1990s the ITU-T consolidated recommendations F.400 and X.400 and published the ITU-T F.400/X.400 (06/1999) recommendation "Message handling system and service overview".