Introduction to Email

Imagine the delight as the first successful carrier pigeon came into land, or the revelation of uncapping the first message-in-a-bottle. Man has come from depending on paper and rock to a world of unending technological possibility – a 40-year cataclysmic shift that has forever altered the how, when, and why of human communication.

For our ancestors, the world was small. Where once face-to-face communication was enough, we now require the ability to communicate across vast oceans. Where once our friends were our neighbors, we now exist thousands of miles apart, friendships and unions that span entire nations.

Before 1971, humanities evolution of its communicative capabilities were, at best, incremental. While man has always been beset by an instinctive need to communicate, it was not until the 19th and 20th centuries that we truly began to expand our tools for doing so. One of the first true long distance capabilities came with the invention of Morse Code in 1836. Experiments on wireless telegraphy began as early as 1830, and in 1947 AT&T first commercialized the Mobile Telephone Service.

However, when Ray Tomlinson sent the first ARPANET email in 1971, the capacity for human communication was forever altered, signaling the advent of true electronic messaging. This first seminal step occurred between two adjacent PCs on the same network, and consisted of nothing more a short segment of text: QWERTYUIOP. Before then, electronic mail systems were confined to a single system, closer resembling a modern day file directory or desktop note application. Simply, they were messages left by previous users for new users to read.

Modern email grew from SNDMSG, a local messaging program that was written by Ray Tomlinson. Tomlinson experimented using a FTP (File Transfer Protocol) called CYPNET to adapt the program, allowing it to send emails to targeted systems on the ARPANET network.

It was at this time that the @ symbol found its place in history. Tomlinson chose the @ symbol to signify to the system which user was ‘at’ either the receiving or sending system.

Evolution of Email

The ‘invention’ of a technology can rarely be pinpointed to a specific date. More often than not, technologies undergo an evolutionary process, incremental steps which, though less significant than other milestones, have nevertheless been instrumental in delivering the email systems we enjoy today.

Obviously, Myspace and Facebook didn’t mark the dawn of social media, but were simply the commercial endpoints to a long evolutionary process.

Here are the milestones, small and large, that contributed to the worldwide phenomenon of email, including the unsung heroes often lost to the recesses of history.

1965 – MIT first introduces email (SNDMSG)

1971 – First network email is sent by Ray Tomlinson over the ARPANET, marking the beginning of modern email.

1977 – Standard format (RFC 733) is considered for enabling email over the Internet.

1978 – 400 ARPANET users receive the first ever spam email for a product demo.

1982 – First recorded use of the word 'email'.

1988 – First commercially available email software, Microsoft Mail, is released for the Mac.

1990 – HTML email first introduced (cue the beginning of the dreaded email spam).

1991 – Tim Lee introduces the World Wide Web.

1992 – Microsoft releases Microsoft Outlook for MS-DOS.

1993 – AOL and Delphi connect their respective systems to the Internet.

1996 – 'HoTMaiL' is launched on July 4 as one of the world's first free web-based email services, symbolically marking the liberation from ISPs.

1997 – Microsoft releases Outlook 97, introducing the core feature set still used today: email, scheduling, contact management, task management, and a journal module.

1997 – Yahoo! Mail is released.

2007 – Gmail is made available to the public.

Current Stats

If there were one million Internet users in 1998 [1]and 2.4 billion in 2012[2], it doesn't take a mathematician to realize that the Internet's lifespan has been one of exponential growth. As one of the core components in the Internet's creation, the same is naturally true of email.

Internet users sent over six billion emails in the whole of 1998. Jump forward 17 years to 2015, this figure has risen to 205 billion per day and is expected to increase by 3% year-on-year until 2019. This includes 122 business emails received per user, per day,[3] and a staggering total of 4.35 billion existing email accounts.[4]

Like the Internet, the adoption rate of email has been rapid and continuous. By the time Hotmail was bought by Microsoft in 1997, it had eight million users. [5]By 2000, this figure had risen to 67 million[6]. Simply, as more and more users had access to the Internet, so did they too to the groundbreaking communicative tools it provided. Email's enormous year-on-year growth essentially correlated to the number of websites being created, the number of users being able to get online, and the ongoing improvements to supporting hardware and software.

---

[1] http://www.adweek.com/socialtimes/Internet-history/475846
[2] http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/
[3] http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
[4] http://www.emailmonday.com/mobile-email-usage-statistics
[5] http://news.microsoft.com/2001/05/14/msn-hotmail-tops-100-million-user-milestone/#sm.00001kr6qzfunnel7upcnyiva9mhp
[6] http://news.microsoft.com/2000/07/17/msn-becomes-top-web-destination-worldwide-with-201-million-unique-users/#sm.00001kr6qzfunnel7upcnyiva9mhp

Protocols

Simple Mail Transfer Protocol – SMTP

Simple Mail Transfer Protocol (SMTP) is the bread and butter of Internet email and the main protocol for sending email messages between servers. It first became widely used in the 1980s and uses push technology with both a store and forward mechanism. Originally defined by RFC 821, it was updated in 2008 by RFC 5321 with Extended SMTP additions.

Today, it is the protocol widely used by electronic email servers to send messages, but not necessarily to retrieve them. Sent messages can be retrieved via an email client that uses either POP or IMAP. Similarly, SMTP is widely used by mail clients to send messages to mail servers, but depends on either POP or IMAP to receive.

Post Office Protocol Version 3 – POP3

Post Office Protocol Version 3 (POP3) is a client and server protocol used by email clients to connect to remote email servers and retrieve and download available client email. It is the primary protocol behind all email communication, and controls the connection between a POP3 supported email client and mail server storing emails.

The first version, POP2, was widely using during the 1980s and required a SMTP to send messages. POP3, however, can be used with or without SMTP.

In the purest sense, POP3 is a store-and-forward service. It is designed to delete emails on the email server once they have been downloaded, although many POP3 clients also possess the option to temporarily store email post download.

Internet Message Access Protocol – IMAP

Internet Message Access Protocol (IMAP) is a standard email protocol that allows users to view, retrieve, and manipulate emails without downloading them. In general, IMAP serves the same purpose as POP3, but offers additional features, including simultaneous access to an email server from multiple devices, better organization through folders, ‘Read’ marks, and ‘Urgent’ prioritizations, and keyword-based search functions.

IMAP was developed in 1986 at Stanford University, and the majority of modern email and webmail systems are IMAP based. Whereas POP3 serves a store-and-forward function, IMAP is typically regarded as a remote file server. IMAP is still used extensively, but has become less important with the rise of web-based email systems, such as Gmail, which have their own interfaces and systems.

How email works

The Process

Each second millions of emails are sent around the world, an intricate web of communication that, if viewed visually, would cover the earth's surface. And yet while our lives very much depend on email, many of us aren't exactly familiar with how it works. Sure, we might know how to send and receive messages, but the simplicity of the end-user experience enjoyed today owes to a hidden network of systems and processes, which together make email the awesome tool that it is.

1. Peter writes a message on an email client, otherwise known as a mail user agent (MUA), and sends it to the recipient's email address.
2. The message, including all attachments, text, and graphics, is uploaded to the Simple Mail Transfer Protocol (SMTP) as outgoing mail. These SMTP servers are also known as MTAs, or Mail Transfer Agents.
3. The SMTP, or MTA, looks at the recipient's address and determines the server destination via the domain name, i.e. the part of the email after the @ (e.g. @gmail.com).
4. Peter's email wanders the world's Internet looking for a home.
5. The SMTP queries the DNS (Domain Name Server) to firstly determine the full domain name of the mail server, and secondly the location. If the domain server cannot be found, the email is returned to the sender with a "Mail Failure" notification.
6. On the other end, the recipient's SMTP server responsible for incoming mail, known as the Mail Delivery Agent (MDA), retrieves and stores the email, and delivers it to the recipient's email box once they log in.
7. The recipient's email client, or MUA, uses either POP3 or IMAP to retrieve the email from the MDA.

So there we have it. Peter's email has found its destination through a series of rapid server connections, creating the instantaneous email experience we're all accustomed to.

Sending Email

Sending an email requires an email client or program. Programs can either be software clients (e.g. Microsoft Outlook) or web-based email programs (e.g. Google). The next bit is down to you: write a message, attach a file, or include a funny picture. The email program will send the message contents, including the subject title, using the associated SMTP.

The SMTP, or email server, dissects the message and identifies all listed addresses in the To, CC, and BCC fields. The SMTP queries the DNS for the full domain name of each address, and the receiving server location. For example, if the address is for @hotmail.com, the SMTP will send the email to the server responsible for the Hotmail domain. For a few precious milliseconds, the email skips about the Internet as it connects to the new SMTP server, which will make it available for the recipient user to receive upon next login!

Receiving Email

So let's say you're receiving an email. Your email program's SMTP, or MDA (Mail Delivery Agent), will retrieve and store any email sent to your address. Upon login, new messages will be retrieved from the server, which is usually the Internet Service Provider (ISP) server, using POP3.

POP3 performs a message carrier function, fetching the email from the server and delivering it to your inbox. The email is now stored locally on your computer, and is arranged within the folder specified by your email client's settings (normally Inbox!).

As we mentioned before, however, sometimes IMAP is used instead of POP3. Unlike POP3, IMAP does not delete an email message from the server post-retrieval until the user deletes the message from their inbox. This is usually the case for web-based programs, such as Gmail and Hotmail, which typically do not store emails on the local computer.

Email, DNS, and MX Records

Emails navigate the Internet using the Domain Name System (DNS), which is essentially a massive, online directory that directs and redirects all email traffic. SMTPs query the DNS when an email is sent for relevant information about the recipient's domain.

This is where the mail exchange record (MX record) comes in. MX record is a type of resource record within the DNS that details the mail server responsible for receiving and storing incoming messages for the recipient's domain. Each domain's MX records instruct how incoming mail should be routed with the respective SMTP.

MX systems allow for multiple servers to be assigned to each domain, and for prioritization to be assigned to individual mail exchange servers. In basic terms, the lowest numbers are given the highest priority. Each server on a list is tried and retried based on their priority until delivery is successful, in order to provide a reliable transmission. In cases of two servers being granted equal priority, each server must be tried before the SMTP may continue down the list. If a domain name returns a list containing only one mail exchange server, the email will be sent to that server regardless of priority.

DNS and MX records are backbone systems in the world's email network, assisting the flow of email traffic, attenuating individual server load, and ensuring email delivery.

Using email

Email Servers (Software)

Mail server software is computer software responsible for the sending, receiving, and processing of messages within the email network. Many of the systems and processes already mentioned, such as MDAs and MTAs, are examples of email server software. Collectively, email server software provides email with Internet message handling services (MHS), and represent different paths and points within the email delivery journey.

Email server software is branded software, and many different versions exist to fulfill each individual function and/or protocol (e.g. SMTP, POP3, IMAP, etc.). Examples of currently popular software performing the SMTP service are Microsoft Exchange Server and Sendmail.

Email Clients

Microsoft Outlook

These days, we have plenty of choice when it comes to email clients. But it was not always so; in the Internet's infancy, email depended on only a few (partly experimental) commercially available clients and programs. One such pioneer was Microsoft Outlook. Outlook's long history extends back to 1992 when it was released for MS-DOS. In these early stages, Outlook lacked the multiple functions, customization, or easy-to-use UI that would become recognized staples of later iterations.

Over its 25-year history Outlook has grown from a rudimentary communication tool to a multi-featured personal information manager – with the inclusion of a calendar, task manager, and contact manager etc.

Outlook was first released to the public in 1997, bundled with the likes of Word and Excel, in what was then and is still now considered to be a revolutionary next step for product software, arriving alongside the seminal Windows 97. At the time of release, Bill Gates stated: "Office 97 marks a great step forward in productivity applications, bringing to business users the benefits of the Internet plus the results of our ongoing research in areas such as natural language processing, user-interface design and software componentization."[7]

Originally, Outlook was only available as an add-on to Microsoft Exchange Server, but was made available to the public with Office 1997 when it replaced the Microsoft Exchange Client.

Mozilla Thunderbird

Before Mozilla Thunderbird's current incarnation and release in 2003, it was originally known as Minotaur. However, once Mozilla Firefox (originally known as Phoenix) began to gain momentum, demand for an associated email client increased, and Minotaur was consequently rebranded and reworked into Thunderbird.

---

[7] https://news.microsoft.com/1996/11/19/microsoft-office-97-released-to-manufacturing/#sm.00000tpfkrs8ukex4zcravzdnzngk

Reflecting a growing trend in software and Internet application development at the time, Thunderbird was released as a free, cross-platform, and open-source email client and newsfeed. From version 1.5 onward, the Mozilla suite was provided as separate applications alongside a new toolkit, which included Thunderbird, deviating from the previous project strategy of an all-in-one suite.

While Thunderbird played an integral role in the development of email clients, and the open-source development community, it has a relatively small market share – used mostly by tech-savvy individuals rather than the average Joe email user. The development of Thunderbird contained many applications and features that would influence competitor clients, but overtime Thunderbird has lost much of its development team and resources, depending largely instead on community input.

Web-based Email Providers (Webmail)

AOL

In 1989 the iconic email pop-up, You've got mail!, first came into use. Two years later, the company behind its creation was renamed America Online Inc., or AOL, marking the birth of one of the most influential Internet and email service providers of the 1990s.

The AOL.com webpage first debuted in 1995 and a year after, in 1996, the AOL messenger service Buddy List was released – the most advanced instant messenger of its day (and for many years to come!).

While the company behind AOL Mail has had a turbulent history, of mergers, acquisitions, and struggling profits (accumulating in a record-setting $100 billion yearly loss), it nevertheless made significant contributions to the evolution of online messaging services and email as a whole.

Originally the AOL Mail and Instant Messenger software was subscription based, whereby users were charged a monthly fee for the service. However, in 2005, each transitioned to the web and were made free-of-charge for users, in part reflecting the industry trend set by the likes of Google and Yahoo!. AOL Mail is otherwise known as AIM Mail, which stands for AOL Instant Messaging, renamed at the time of its incorporation into a webmail service in 2005.

Unlike AOL Mail, the 2005 incarnation did not require software for use, and was available simply by logging onto the mail.aol.com website. AIM Mail was originally released with 2MB of available storage per user, which was the highest available at the time. Today, AOL offers unlimited storage for all AIM users, and a free @aol.com email address can be setup by visiting the mail.aol.com website.

Yahoo!

Yahoo! was founded at Stanford University in 1994 by Jerry Yang and David Filo. Yahoo! grew exponentially throughout the 1990s, first becoming a web portal before extending its service offerings with a series of high-profile acquisitions, which included Four11 in 1997. The acquisition of Four11's Rocketmail webmail service was the beginning of Yahoo! Mail, which officially launched later that year.

Yahoo! Mail has gone through several different iterations, and up to three versions of the web-based UI were available at any given time, accommodating new and old users alike,

with the original 1997 version available until 2013. A beta version of Yahoo Mail was introduced in 2010, which became the default interface in 2011, and brought a number of UI improvements, customization options, and integration capabilities (Facebook etc.). Yahoo Mail has been continuously improved since, with a repeatedly simplified design and added features. The latest version was released in 2015.

Yahoo! Mail has had unlimited storage since 2007. It currently has an estimated 300 million users. The latest version includes the ability for users to switch between email, chat, and text messaging, for an all-inclusive communication service. Yahoo Mail accounts are free for personal users and require only a Yahoo ID, which can be setup by visiting the mail.yahoo.com website. Yahoo Mail also offers a paid service called Yahoo Mail Plus, which offers additional features.

Hotmail

Hotmail is a free, web-based email service from Microsoft. Not to be confused with the email client Microsoft Outlook, Hotmail, or outlook.com, was founded in 1996 and originally sported a funkier variation of its name: HoTMaiL (with all the capital letter placements in-toe). The name was changed to its current form when the service was bought by Microsoft in 1997, officially becoming MSN Hotmail.

Hotmail was one of the first free web-based email services and was highly influential in the development of the service type. Significantly, it was the first to develop and offer safety innovations, including automatic anti-virus scanning, as well as an integrated calendar, spell checking, and a web messenger.

Eventually, in 2007, MSN Hotmail was replaced by Windows Live Hotmail, a move in part motivated by the emergence of new market competition a few years earlier, namely Google and Yahoo!. Over the years Microsoft made ongoing improvements to its service, including speed and security improvements, optimization for new browsers, added features, and extended storage space.

Outlook.com beta was first introduced in 2012. The service was officially deployed on April 3 2013, at which point existing Hotmail users were forcibly upgraded to the new outlook.com web service, but allowed to keep their existing Hotmail addresses (with the option of replacing the @hotmail.com domain with @outlook.com). According to Microsoft, outlook.com had over 400 million active users by May 2013.

In 2015, Microsoft announced plans to migrate the outlook.com service into the Office 365 infrastructure. This included the introduction of a number of new futures, with additional benefits available to Office-365 subscribers. Outlook requires a free Microsoft account to access, which can be setup by visiting outlook.com.

Gmail

Gmail was first released in beta in 2004, and became available to the public in 2007. It is demonstrably the most widely used free web-based email service, and certainly has become the most well-known.

By 2004, Google had already established itself as the search engine kingpin, but few could foresee the momentous feats still to be made by the company, forever reshaping the landscape of Internet services. In fact, and in no small part owing to the April 1 announcement date, many were initially incredulous of idea that Google, a search engine

provider, was about to release a web-based email service that not only threatened the dominant market positions of Hotmail and Yahoo!, but promised to eclipse them entirely. It was faster, no longer requiring full page reloads for each new page, sleeker, with the first instant search capabilities, and had a groundbreaking 1GB in storage, no less than 500x that of Hotmail.

George Harik, Gmail's lead developer, succinctly described the menagerie of disbelief and hype experienced at the time: "If you're far enough ahead that people can't figure out if you're joking, you know you've innovated."[8]

While the 2004-2007 period was officially Gmail's beta, it was, in reality, more of a stinted release. From 2004 Gmail was being made available to the public incrementally, through mounting waves of invites. The initial hype surrounding Gmail did not abate even with its eventual official public release in 2007, and beta invites were regularly bought and sold on open market websites, such as eBay.

Unlike Yahoo and Hotmail, Gmail has survived with its original architecture. While there have been continuous updates, polishing, and added features, such as Google Chat, VOIP support, spam filters, and social media integration (including Google+), the Gmail we enjoy today is essentially the same as the one released in 2004.

Gmail changed the face of web email, largely bridging the QoE (Quality of Experience) that had previously existed between web-based services and local email clients, setting a new precedent for its competitors to follow. A free Gmail account can be setup by visiting gmail.com.

Webmail Software (Clients)

First, it's important to make a distinction between webmail clients and webmail providers. What we've just discussed are examples of webmail service providers – the likes of Gmail and Yahoo – which provide email access via a webmail interface.

Webmail clients, on the other hand, are responsible for sending and receiving email messages through local or remote servers. Like local email clients, webmail clients root messages through POP3 and SMTP protocols. A webmail client can be understood as any email client made into a web application, running on a web server, or as a gateway interface that permits access to one or more IMAP or POP3 email accounts through SMTP.

Horde

Horde is a free, browser based, fully-featured communication suite, comprising various PHP-based applications. Horde evolved from IMP (Internet Messaging Program), a webmail client able to access emails stored on IMAP servers and one of many applications currently contained within the Horde Groupware.

In total, the Horde Groupware Webmail Edition consists of eight separately available applications: IMP, Ingo, Turba, Gollem, Trean, Mnemo, Kronolith, and Nag. Each application serves a function of the framework, for example, providing support for calendar, notes, tasks, IMAP and POP3 email access, and file management. Horde features different

[8] http://time.com/43263/gmail-10th-anniversary/

interfaces for each connected device with cross-platform synchronization, making it accessible from anywhere (device permitting!)

Horde is an open source project, which basically means it is continuously in development, evolving alongside community need. Horde permits users to access, monitor, and organize multiple webmail accounts at the same time. Through a single interface, the user can send and receive email messages from and for each email account simultaneously, with all modern email features and customizations present (HTML, drag-and-drop, spell checking, filtering, etc.)

SquirrelMail

SquirrelMail is a free, open-source webmail package that includes both a PHP-based webmail client and proxy server for the IMAP and SMTP protocols. The original webmail client was created in 1999, and can access any IMAP email server account (requiring both the IMAP server responsible for hosting the email and a SMTP server to send and receive messages).

The SquirrelMail webmail client features a simple and straight-forward interface, paired with basic email functionality such as a calendar, spell check, attachments, address books, and text-only composition. In comparison to most webmail clients, including Horde and RoundCube, SquirrelMail is one of the simplest, easiest to setup, and most practical.

SquirrelMail uses a plugin architecture, allowing for additional features to be added alongside the core application, with over 200 plugins available through the SquirrelMail website. All of SquirrelMail pages are rendered in HTML 4.0, enabling cross-browser support, speedy loading, and ease of use.

Roundcube

Roundabout is a browser based, open source IMAP webmail client that uses Ajax technology – a set of web development techniques used to create asynchronous web applications. In terms of features, Roundcube sits somewhere between SquirrelMail and Horde, with the full functionality expected from a webmail client, including folder organization, search, MIME support, address book, spell checking, cross-browser support, and multi-lingual capabilities.

The first release of Roundcube came out in 2008. Since then, and owing largely to the open-source community, it has received numerous updates and UI refinements. The client simulates a desktop-like user interface to provide ease of use and configurability. It is known among users for its user-friendly, clean, and fully customizable UI. Like SquirrelMail, Roundcube requires both the user provider's IMAP and SMTP servers to send and receive email messages.

In May 2015, Roundcube Next was announced – a complete rewrite of Roundcube with additional features to be added, such as a calendar, chat, and file management.

Tips

Username Selection

Selecting a username is a right-of-passage for a first time Internet user, and a matter of careful consideration anytime thereafter. Suffice to say that username selection is a task that should never be taken lightly; from security to professional appeal, the differences between a good and a bad username can have a huge impact on your email life, whether professional or social.

Firstly, it goes without saying that a username should be easy to remember, personal to you, and not too unusual or out-of-the-ordinary for others. Nicknames, for example, can be problematic when used as usernames. While all your friends might know you as 'pandabear', such a name will appear unprofessional and strange to others (as well as having little to do with your real name and identity!).

So, the main criteria to keep in mind is to have a username that is firstly unique, and secondly practical and professional. Otherwise, here are some basic tips to keep in mind when choosing your username:

1. **Make it about you.** Try to use your username as an identifier. It doesn't have to be your real name, but it should be a name for which you are commonly recognized. Naturally, it's logical for a company's email to use the company name. Feel free to be creative and make it unique, but be careful of anything profane, rude, or otherwise alienating.
2. **Adding numbers.** If you use numbers, make sure they're numbers you're going to remember (such as the year that you or a family member was born).
3. **Avoid prefixes and suffixes.** When choosing a username, stick to nouns, avoiding adjectives such as 'awesome' added before or after the name.
4. **Bypassing already taken usernames.** If your desired username is taken, play about with slight variations. However, don't go too crazy with adding extra numbers and letters, which will result in a convoluted name that is too hard for either you or others to remember and identify.

Using Your Own Domain

An email username isn't the only way to personalize an email address. You can also create custom domains, which is everything after the @ symbol. Custom domains are commonly used by companies and groups to easily identify users that belong to their organization. However, they're also used by individuals who wish to brand themselves (much like a written logo), or have a more professional and unique email address.

There are various ways to acquire a custom domain, including self-hosting (via a local server), third party email hosting, or purchasing one from one of the main email providers (such as Google). Alternatively, there's the option of using an email address provided via your local ISP, or Internet service provider. However, this is generally not advised as ISP email addresses are, by their nature, static. Since we're all meeting and exchanging our addresses every day, it's important that our email accounts remain accessible regardless of location.

Alternatives to creating a personal email domain include:

1. **Email provider hosting.** Email providers such as Google and Yahoo offer custom domains (usually with a monthly fee). The domain will be hosted on the respective provider's email servers, and will enable the user to access their account through the same method as a generic domain account. As part of the provider's service, custom domains often come with additional bonuses and perks, such as the ability to add additional users under the same domain.
2. **Hosted email.** There are a bunch of email platforms available that allow you to easily host your own domain. The benefit of this is that it requires far less technical know-how, and makes managing your domain easy through clean and simple interfaces. The top market providers of hosted email services include Zoho Mail, Fastmail, and Rackspace Email.
3. **Email forwarding.** If you're after the branding advantages of a custom domain but don't want to venture into unfamiliar territory, email forwarding is a smart alternate to the above. Through the likes of Pobox, a service that specializes in email forwarding, messages sent to your unique email will be forwarded to the email platform and address you're accustomed to. For example, if you're currently using an @yahoo.com address but want to receive messages to a @homebusiness.com domain, Pobox will forward all messages sent to the new address to your usual account, from which you can reply and send messages as normal.

Email Etiquette

Yes, there is such thing as email etiquette. The Internet is hardly a civil place at the best of times. We are, after all, living in the age of the Internet troll. However, emails have always been quietly exempt to the usual barren lawlessness that presides over the likes of forums and YouTube comment sections. Everything sent via email is tracked, permanent, and, in many instances, legally binding.

We have the reliability of email communication to thank for much of this. As providers cemented their foothold in the world of online communication, email storage sizes increased, eventually leading to the birth of cloud storage. Basically, everything we send or receive is often logged onto our accounts for a long time – a diligent recipient can pull up an email after five years with your signature, reminding you of a commitment you'd so blissfully forgotten.

In many ways, what we write in emails is more important than what we say, or how we speak. Anything written can be used against us. And given that most professional communication now transpires through email, how we write them is a significant part of how we come across to our peers.

1. **Avoid capitals.** Meeting somebody for the first time and shouting at them is never a good idea. The reaction would be the same for an email written in capital letters. Capital-strewn emails tend to create a negative impression, and are ultimately irritating to read.
2. **Tone down the Internet slang.** We all love our acronyms, text speech, and emoticons, but overuse can be damaging to our emails. Of course, much of this depends on context and whether you're sending an email to a friend or a coworker. In cases of the latter, throwing in a 'lol' after every sentence is always going to look

bad, while emoticons pose the risk of appearing overly familiar and informal with the recipient. Basically, don't use sticky-out-tongue faces with your boss.

3. **Avoid requesting read receipts.** If you've been the victim of mounting read receipt requests, you'll have a solid appreciation of just how annoying it can be. While professionally it is sometimes necessary (and often tempting) to request read receipts, overuse of the feature tends to result in more irritation and less productivity.
4. **Watch out for confidential information.** In one way or another, everything written in emails is permanent. Ergo, nothing written is ever truly safe, and all email content poses the risk of being leaked or seen by unintended eyes. Confidentiality is a major issue within Internet and email security. As a basic rule of thumb, don't write anything that you wouldn't want others to read. There is mounting legal legislation surrounding email communications. What we write, even in the heat of a moment, can be used against us; we are equally accountable to what we write as to what we say.
5. **Keep it clear, correct, and to the point.** It goes without saying, but a good email should be well written. It's best to avoid an overuse of exclamations (such as ?!?!) and to write to the point, conveying exactly what you intend to say. This includes a clear subject line.

Email marketing

History

Ray Tomlinson's vision for email was simple: to enable networks to be able to communicate with one another, wherever they are. Two decades later, the evolution of email began a new tangent into the world of email marketing, uncapping the online potential for commercial outreach and customer acquisition.

Email was no longer a tool exclusively for socializing and professional communications, but a lucrative avenue for commercial outreach and customer acquisition.

Email marketing is the natural successor to postal marketing. For our parents and grandparents, a daily trip to the mailbox (the real one that sat on the end of the drive) promised a trove of promotional pamphlets, brochures, and flyers. This regular bounty of marketing treasure was naturally expensive for companies to produce, and the approaches used to target potential customers were rudimentary at best. Email marketing is cheaper and far more effective than anything that has come before, or since. Texts, instant messengers, and even social media are or have been incredibly powerful marketing tools, but they exist as off-shoots to what is now the core pillar of 21st century marketing: email.

Email enables direct, one-to-one communication with customers. The ROI (Return of Investment) potential is momentous, and the growth in users' daily email use shows no signs of abating. In fact, the growth of email marketing can be directly correlated to the growth of the Internet, the technology available, and the birth of the mainstream email providers we're already discussed. Throughout the seminal 90s (and starting in 1991 with the World Wide Web Project) email providers such as AOL and Hotmail were sprouting up, offering new and amazing ways to communicate with mass audiences. In these early days, email marketing became more bane than boon for the average user; promotional emails mostly took the form of spam, a rudimentary attempt to throw countless messages at any available ISP in the vain hope that one or two would be opened.

By the start of 2000, the number of email users was skyrocketing. In 1998, the Data Protection Act was updated to ensure companies provided an opt-out option for email recipients. Later, in 2003, the Can Spam Law was introduced in the US to regulate commercial emails, and in 2004 the European powers introduced the Privacy and Electronic Communications Regulations, which first set out a bunch of rules for the dos and don'ts of online marketing.

Email marketing's produce has been commonly maligned with spam. While there's some truth to this, and has been for much of email's time in the limelight, it's been less the case since the advent of social media. To put it simply, social media has normalized the selling of commercial products within social spaces, while the advancements made in email filtering has helped divide good spam (the sort of things you might actually be interested in based on search and purchase histories) and bad spam (random floods of emails crammed through the banks of each and every ISP).

From sponsored emails and newsletters to a whole slew of lead conversion techniques, email is a virtual goldmine of opportunity for any budding marketer.

Top 10 Email Marketing Services

The secret of email marketing's amazing profit returns is not much of a secret. These days, every company wants a slice of the lucrative email pie – to be able to make one-to-one connections with their customers and pick up a bunch of new ones along the way. However, while the want and need is certainly there, businesses often find themselves unable to execute an effective email marketing strategy. Luckily, various marketing services now exist to help businesses achieve just that, removing the fiddly know-how of mass email marketing with clear and intuitive interfaces, leaving behind only the onus of creating catchy, eye-grabbing content and the age-old joy of A/B testing.

1. **Campaign Monitor.**

Campaign Monitor is a hugely popular email design software, allowing the user to create effective, attractive emails through an intuitive interface, featuring drag-and-drop capability and a host of style options. Users also have plenty of tools for optimizing their outreach, sending specifically targeted email campaigns to desired locations and demographics.

2. **Mad Mini**

Mad Mini lets you design and customize your own HTML email templates. The mainstay of the software is its collection of themes and styles that enable users to tightly tailor their campaigns for each target audience. The software features report and tracking and robust management capabilities, allowing for effective A/B testing and statistic-backed optimization.

3. **Benchmark Email**

As the name suggests, Benchmark Email is all about optimizing the effectiveness of email campaigns. It offers a set of tools for enterprises to maximize their outreach and devise results-driven strategies, with reporting to show the quantity of opened emails, A/B testing to compare different emails' effectiveness, and list management to build a portfolio of targeted customers.

4. **MailChimp**

Created in 2001, MailChimp is one of the more seasoned email marketing services, featuring a drag-and-drop block designer with a collection of email templates that can be easily customized. Additional features include robust automation capabilities, analytics, and integration with a wide range of platforms, devices, and apps.

5. **GetResponse**

GetResponse software prides itself on its simplicity and selection of design options, with customizations for a variety of email types and Internet pages, including landing pages and forms (and even the ability to design your own Webinar!).

6. **iContact**

iContact is a cloud-based email marketing software. It's won a bunch of awards since its creation in 2003, and comes with a wide range of tools suited for both beginners and advanced users. Features include robust automation options, result tracking and analytics (with integration to major CRMs), and design options for both emails and landing pages.

7. **Campaigner**

Campaigner's primary focus is on email automation – enabling users to develop thorough conversion strategies to maximize customer interaction. Features include reporting and analytics, automation, SMTP relays, and A/B test monitoring.

8. **Graphic Mail**

Graphic Mail is an email marketing platform built for designers. Naturally, this means it's a great choice for creating fancy looking and effective emails, with a slick and easy-to-use interface that allows for some interesting (and effective) creations. Features include drag-and-drop, a range of pre-existing responsive templates, dynamic IP pools, and real-time delivery stats.

9. **ConstantContact**

ConstantContact offers email marketing services for the everyman – from small business owners to large companies. The service includes a collection of stylish templates, which can be easily customized to fit the needs of each business and target audience. Meanwhile, standard features include contact list management, automation for outgoing mail, based on pre-set criteria and schedules, and reporting and analytics.

10. **StreamSend**

StreamSend is an all-inclusive email and social media marketing platform, enabling companies to develop cross-channel marketing strategies. It offers a range of delivery and optimization tools, easily manageable with a simple and clean UI. Additional features include automation, image hosting, a database of customizable email templates, and reporting and analytics (for both social media and email).

Tips & Tricks

Early email marketing was mostly a case of scurrying around in the dark – an attempt to discover the elusive mechanisms that would make customers want to buy a service or product.

Implementing effective email marketing strategies is never a straight-forward process. The first trick is to follow a set of assumptions. Assumptions are necessary when targeting a specific target audience – what you write, design, or create must mirror the needs and tastes of the recipient, and appeal to their sensibilities. Obviously, emails intended for teenagers and adults are going to differ significantly in their style and tone. In email marketing, one size never fits all.

Other necessary assumptions relate to success. Each and every email user receives up to and over 100 emails per day. Many of these are promotional emails, all vying for the individual's attention. Your email must be specifically targeted, relatable, and have something the individual wants. Understanding your target audience is key. Secondly, mass email naturally means that many of your emails will not be read. A/B testing exists not to ensure that every recipient reads an email, but that the highest possible number of recipients do so.

1. **Write simple. Super simple.** Straight forward and to-the-point writing achieves better results than overwritten, convoluted paragraphs. Emails require a quick and attractive pitch, delivering a concise message that will capture the reader's attention. This is also very true of an email's design.

2. **Keep it informal.** A great advantage of email is the one-to-one connection. The world of Internet marketing is one of relatability, bridging the gap between company and consumer once and for all. Formal introductions aren't required. Talk with your audience, not at them.
3. **Avoid excessive compliments and embellishments.** It's nice to have customers feel good about themselves, but continually congratulating them for having initiative, for example, can damage an email's success. Email users are becoming more and more savvy, and an over-complimentary email can stink like moldy cheese.
4. **Make it interesting and personal.** Recipients are quick to make decisions about the emails they do or don't read. Subject lines and first lines matter, a lot. In many instances, this will be your only chance to convert a potential customer into an actual customer. An email marketer's best skill is to make an email personal without using the recipient's name.
5. **Test, test, test.** Optimization is the name of the game. Many email campaigns fail, but their failure should never be written off. Most email services offer ways to monitor the success of emails alongside A/B testing features, through which lessons can be learnt. Emails should always be refined versions of their predecessors (until you hit the mark!).

Email security

Security threats

As great as the Internet is, it can become a bit like the Wild West – there are plenty of people out to abuse its security, infiltrate accounts, and generally ruin everybody's good time. It's fair to say that when the APRANET was first conceived, the thoughts of the few early adopters were more on pioneering the future of communication technology, and much less on security. After all, with only a hundred or so users, it wouldn't be hard to trace down the culprit of any security breach.

Flash forward to the modern day, however, and security has become a major (if not the main) issue facing Internet use, affecting individuals, companies, and governments alike.

Spam

Spam is the unwanted knock on the door on a sunny afternoon, or the unending onslaught of phone calls that we're just unable to ignore. Spam grew up as email's conjoined evil twin, becoming a vehicle for malicious attempts to scam unsuspecting users and flog products with dramatically embellished benefits, such as the ability to grow multiple limbs or turn back time.

But not all spam is bad. Improved spam filters have proven to be a double edged sword for marketers. While they protect the average user from an avalanche of unwanted email, they also create barriers to mass email, especially within the email marketing arena. After all, one man's junk is another's gold.

Statistics

While the number of sent spam emails is technically growing, the percentage of spam to normal emails is, in fact, decreasing. The security technologies used in email clients are miles ahead of where they were a decade ago, and most spam fails to even enter our mailbox. In fact, when counting the spam that successfully entered inboxes, the average email user received 12 spam emails per day across 2015, out of a total average of 122.[9] Only 10% survive their journey through the email filters, and of those 10% only half are ever opened by the user.[10] More pertinent (and shocking) statistics include:

- 89% of all emails sent in 2011 were spam, accumulating in a total of 260 billion spam messages.
- 88% of spam is sent from botnets (compromised computers).
- 69% of email recipients mark email as spam based on the subject line alone.
- 66% of all spam is about selling pharmaceutical products (multiple limb potions etc.).
- Only 0.7% of spam is sent from known email providers (Gmail and the like). [11]

[9] http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
[10] http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx
[11] http://royal.pingdom.com/2011/01/19/email-spam-statistics/

ACMA, CASL, 2002/58/EC, CAN-SPAM (Act of 2003)

Different countries have introduced different legislations to counter the spam problem. Naturally, this has made a marketer's job more complex, especially for those that boast an international contact list. Nevertheless, regulation is a necessary and pertinent step for the world of email, making the Internet a safer place overall.

ACMA

The ACMA is the Australian authority responsible for enforcing the 2003 Spam Act and overseeing all of the country's communications. The Spam Act prohibits the sending of unsolicited commercial emails that originate from or are accessed within Australia. In a nutshell, the Spam Act dictates that any digital communication should be sent with consent, contain sender identification and contact information, and include an opt-out option.

CASL

The Canadian Anti-Spam Legislation (CASL) is the better known name for the Fighting Internet and Wireless Spam Act (FISA), which came into effect in 2014. CASL is notorious for being one of the more stringent anti-spam legislations. It dictates that marketers can only send emails to those who have expressly consented to receive messages, such as subscribers, or have provided implied consent through previous purchase of a product or service.

2002/58/EC

The 2002/58 directive on Privacy and Electronic Communications (EC) is an EU directive that covers data protection, privacy, and spam. 2002/58/EC came into effect in 2002 and was drafted as a response to the emerging digital technologies, such as electronic communications, in order to protect personal data. The directive builds on previous data protection legislation, namely the Data Protection Act of 1998. While it covers a range of communications, it had an early significant impact on email, dictating that emails must be sent only with the recipient's prior agreement (known as the opt-in regime) and must include an opt-out option. The restriction does not cover implied consent or existing customer relationships that are established through previous purchases.

CAN-SPAM Act of 2003

The 'Controlling the Assault of Non-Solicited Pornography and Marketing Act' is the US's main anti-spam provision. Better known as CAN-SPAM (because the full name is a mouthful), the act was introduced in 2003 to establish a basic set of rules for all commercial email communications. Enforced by the Federal Trade Commission, the act includes such provisions as the prevention of misleading information, requiring the sender to include all originating information and clearly identify their business and purpose, information on how to opt out of communications, and the prevention of deceptive subject lines.

Viruses

When users think of email, the thought of computers viruses won't be too far behind. Viruses have plagued the good name of email for decades, turning vulnerable inboxes into proverbial minefields for the unsuspecting user.

Email viruses are typically simple, and involve tricking the user into downloading an attachment, either directly or through a link. Well-known (and destructive) email viruses

include the Melissa virus in 1999, which spread via Microsoft Word documents sent through email, and the ILOVEYOU virus in 2000, which contained a piece of code that when clicked on would execute the malignant virus program. A more common day-to-day threat is from malware, which functions in a similar fashion to the above (and other forms of Trojans). A shocking 64% of users have at one time been the victim of malware infiltration through email. [12]

Phishing and identity theft

The definition of phishing isn't too dissimilar to what its homophone, fishing, would imply. Phishing involves malicious attempts to acquire sensitive information, such as social security numbers, credit card numbers, or addresses, in order to gain access to financial accounts or, as is often the case, steal identities. Phishing scams are executed en masse through millions of emails, collected from a variety of sources. Hence the fishing part; the scammer's intention is to trick a handful of people out of hundreds of thousands.

Obviously, if somebody tried the same trick in broad daylight, the response would be a resounding no. However, phishing scams can be incredibly sophisticated, often substantiated by elaborate back stories and attempts to establish validity (with emails and websites that closely resemble those used by official institutions, for example, such as banks). In nearly all cases, they will involve a request for personal information, either directly or through a bogus website masquerading as an official login page, but can also involve bank transfer requests.

Well-known phishing scams include a Nigerian prince asking for assistance reclaiming his inheritance, and suspension notices from entities masquerading as eBay, requesting that the user follow a provided email link and update their credit card information.

Solutions

Preventing and filtering spam

Luckily, it's a lot easier to prevent and filter spam than it was a decade or so ago. Many email providers have in-built spam prevention mechanisms, which will automatically categorize email as spam if it falls within predefined criteria or originates from an unknown or blacklisted address.

Whichever way you're accessing email – whether through a software or webmail client or an email provider – make sure there are in-built filtering options available. Most email software features advance filtering options. Windows Live Mail, for example, allows the user to switch between 'standard' and 'exclusive' filtering presets. In case of the latter, only email that is from a listed contact or registered safe sender will be permitted into the user's inbox.

Otherwise, spam that successfully infiltrates your inbox should be immediately flagged as junk mail. Spam can be identified by carefully observing aspects of the email. For example, a recipient's address will not be present in either the To: or CC: fields, or the email's subject line will contain strange characters or a surplus of spaces (which are sometimes used to hide identification codes from the recipient). Flagging an email as junk will also automatically

[12]http://www2.trustwave.com/rs/trustwave/images/Best_Practices_in_Email_Web_and_Social_Media_Security_Trustwave.pdf

send future communications from the sender's address to the spam folder. Other helpful prevention methods include:

1. **Look, but don't click.** Usually, it's easy enough to identify a suspicious email from the address of the sender. For example, an obvious sign is when an email has slight, out-of-the-ordinary character variations, especially from well-known or trusted emails (e.g. accounts@ebayaccounts.com).
2. **Spelling mistakes.** An obvious one; a lot of spam originates from non-English speaking countries, and a surplus of spelling mistakes is often part of the spammer's package.
3. **Play it safe and don't click on any links.** If you're even remotely suspicious about the validity of the email, play it safe. Malicious links can not only lead to fraudulent websites, but also to the unintentional downloading of an email virus or malware. The same goes for attachments.
4. **Analyze the content.** From the salutation to the body of text, analyze to test for inaccuracies or suspicious language. For example, if the salutation is addressed to a non-specific individual, it's safe to assume they have no idea of either your name or gender.

Encryption

Encryption is a great way of safeguarding sensitive information from rogue parties or unintended eyes. While it's much harder to infiltrate (hack) accounts than it used to be, there are still a variety of ways that your password can be compromised, either through key logging (software hidden on your computer that records password entries) or by simply not having enough character variation (known as the 'strength' of the password).

And even greater dangers exist in third party monitoring of our communications. We trust our emails with a lot of sensitive information. The fear that prying eyes might have sight of such information during transit is a very real one.

There are several third party plugins that enable client side encryption (i.e. before the email has been sent). Web services like Mailvelope allow webmail users to encrypt text prior to pressing Send, paired with both a public and private decryption key (which must be used to decrypt the message). On the other hand, PGP (Pretty Good Privacy) is a popular encryption choice for local email clients, using the OpenPGP standard for signing, encrypting, and decrypting texts. Alongside the likes of S/MINE and ProtonMail, PGP is a form of end-to-end encryption for email, which is regarded as the most secure form of encryption as no entity along the delivery pathway, including ISP providers and service operators, can view the content.

Most popular email software, including webmail, also has in-built encryption options for outgoing email in transit. Microsoft Office, for example, allows the user to select to encrypt all outgoing contents, including attachments, through its Tools menu. Gmail, meanwhile, uses TLS as standard to secure all outgoing communications. TLS (Transport Layer Security) exists as another layer to the SMTP connection, protecting email content as it travels between SMTP servers.

Security practices

Email isn't all doom and gloom. The nasty side of email is the exception to the easy, smooth, and pleasant experience most of us enjoy every day. Technology is constantly improving to

protect unsuspecting users, and generally the Internet-using population is becoming more savvy to the tactics and tricks employed by malicious parties.

Still, a user should never let their guard down. Here are a number of practices we recommend for that extra layer of security:

1. **Use email that has TLS encryption.** TLS encryption is becoming the standard, but requires both sender and recipient to have a TLS-enabled client for it to function as intended.
2. **Unknown equals uncertain.** Don't take chances attachments or links. If the sending address is unfamiliar to you, simply ignore the message and its contents.
3. **Protect your address.** Like telephone numbers, email addresses shouldn't just be given to anybody who asks. Many websites will request our email address for special offers, or to provide limited access into restricted parts of a website. Do so with great consideration – many third parties will attempt record our address for spam lists, or sell on to other third parties.
4. **Limit sensitive information.** If the worse happens and your emails are compromised, sensitive information will become exposed. Information such as bank account login details or credit card numbers should never be contained within an email. Likewise, sensitive or embarrassing information should be sent sparingly.
5. **Complex passwords.** While it can be a pain to remember complex passwords, they are necessary for safeguarding email accounts. Don't use names or predictable words; the best passwords are a random combination of different letters, numbers, and symbols, which would be impossible for a hacker to guess or key logger to identify. Likely, don't store your password anywhere on a computer or cloud storage, which includes 'note' applications.

Sources

Cook, R. and Cook, G. (2011). *Guide to business etiquette*. Boston: Prentice Hall.

Jenkins, S. (2009). *The truth about email marketing*. Upper Saddle River, N.J.: FT Press.

Paulson, M. (2015). *Email Marketing Demystified: Build a Massive Mailing List, Write Copy that Converts and Generate More Sales,* American Consumer News, LLC.

Sunner, M. (2005). Email security best practice. *Network Security*, 2005(12), pp.4-7.

Osterman Research, Inc., (2016). *Best Practices in Email, Web and Social Media Security*. Washington: Osterman Research, Inc.

Jordan, S. (n.d.). *From smoke signals to email*.

White, C. (2014). *Email marketing rules*. United States: CreateSpace Independent Publishing Platform.

Flynn, N. and Kahn, R. (2003). *E-mail rules*. New York: AMACOM.

Groves, E. (2009). *The Constant Contact guide to email marketing*. Hoboken, N.J.: Wiley.

Gralla, P. (2007). *How the Internet works*. Indianapolis, IN: Que Pub.