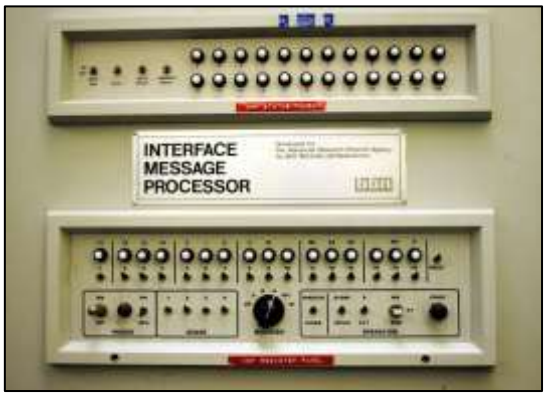
Allan George's Gems

The birth of the Internet.

Charles Kline's first attempt to send a message over the Advanced Research Projects Agency Network (ARPANET), the early computer network that would birth the internet as we know it, was a bit of a dud. Sitting at his massive mainframe computer at the University of California, Los Angeles, the grad student sent an "L" to another apartment-sized machine at Stanford University. Then an "O" but before Kline could get to the "G" in his attempt to send the word "LOGIN," the system crashed. He would revive the connection later that night and successfully transmit all five letters, but it wouldn't matter if he hadn't. He had already made history.



On October 29, 1969, "LO" was the first message successfully sent over a computer-to-computer network.

It would be another decade before ARPANET gave way to the internet and another decade after that before the World Wide Web was born. Before those revolutions could be realized, two major questions had to be answered:

- How could ARPANET expand, and
- what the hell were people supposed to do with it, anyway?

The first problem was addressed by internet icons like Vinton Cerf, who developed the protocols that would allow different networks to connect to one another and form a larger network of networks. (In other words, an "internet.")

Ray Tomlinson worked on the second problem. In 1971, in search of a “more convenient and functional way to communicate,” Tomlinson tapped out a message on one hulking DEC-10 mainframe and sent it to another.

He’d invented a ground-breaking new system of communication. While he didn’t call it email, he did separate his name from his location with the @ symbol. New networks sprouted up across the U.S. in the 1970s, with government agencies and educational institutions signing their networks onto the internet. In 1974, the first public ISP, Telenet, was launched but the internet of the ‘70s was still largely the realm of those with the technical know-how to navigate early operating systems and access to machines running them.

That all began to change in the ‘80s with the advent and spread of the personal computer, dial-up access, the domain name system, and USENET, a precursor to web forums. Then in 1990, we crossed the Rubicon. The past was closed off, as ARPANET shut down and the future opened, with the creation of the World Wide Web.

By the end of the decade, the internet and the web became synonymous as millions of people got online to chat, shop, learn, discuss, innovate, meme, and read lists. To properly tell the story of how the internet grew, here are several sites that made it what it is today: a wonderful, weird, occasionally terrible, but always transformative place to be.

CERN. 1990

December 20, 1990 didn’t feel historic at the time, but it was the day a British computer scientist in the Swiss Alps published the first-ever website at the European Organization for Nuclear Research (CERN). From his NeXT computer, Tim Berners-Lee published, appropriately enough, a primer on the web, explaining the concept of hypertext and describing how to set up a server. But Berners-Lee didn’t share the site with the public until a year later, when he told his friends in

the alt.hypertext newsgroup about his creation. It would take another couple of years and the arrival of the first “killer app”—the browser Mosaic—for the web to catch on.

AOL 1993

For many Americans AOL.com served as their introduction to the web. After the whirring and beeping of their dial-up modem mercifully ended, they were greeted with a one-stop-shop that let them browse headlines, read horoscopes, and check their “mail.” It was magic, but by the mid 2000s, after AOL’s disastrous merger with Time Warner, AOL.com had become a relic. With a decade of experience, web users had grown savvier and less reliant on portals to find their way to the content they wanted.

Amazon 1994

Jeff Bezos knew he wanted to start an e-commerce business before he knew what he wanted to sell. After researching the biggest mail-order businesses in the country, he settled on books, a product with too much variety for any store to stock completely. By 1996, Amazon was making millions selling books through its straightforward website that offered some of the same services it does today: reviews, recommendations, and a vast inventory. Before long, Amazon had expanded to music, movies, clothing, household items, and ultimately everything else on the planet, even web hosting, hardware, and robotics. It has evolved to consume a bigger and bigger chunk of e-commerce and in 2018, the retail giant accounted for 37 cents of every dollar U.S. consumers spent online.

C

Chuck Norris's keyboard doesn't have a Ctrl key because nothing controls Chuck Norris.

Yahoo 1994

When Yahoo launched in 1994, it wasn't called Yahoo and it wasn't a search engine. "Jerry and David's Guide to the World Wide Web" was a web directory maintained by hand that provided links to a much smaller internet than we have today. Major changes came within a year. Jerry (Yang) and David (Filo) changed the site's name to Yahoo and introduced a tool allowing users to search the directory. By 1998, Yahoo.com ruled the web, with close to 100 million page views a day. Many acquisitions followed over the years with Yahoo buying GeoCities, Broadcast.com, Tumblr, and others but few were successes. While Yahoo's business fortunes have sometimes suffered, Yahoo.com still remains one of the most popular websites on the internet.

Maybe the portal model is dead but if it's combined with a competent search engine and a popular email service, maybe it can live forever.

eBay 1995

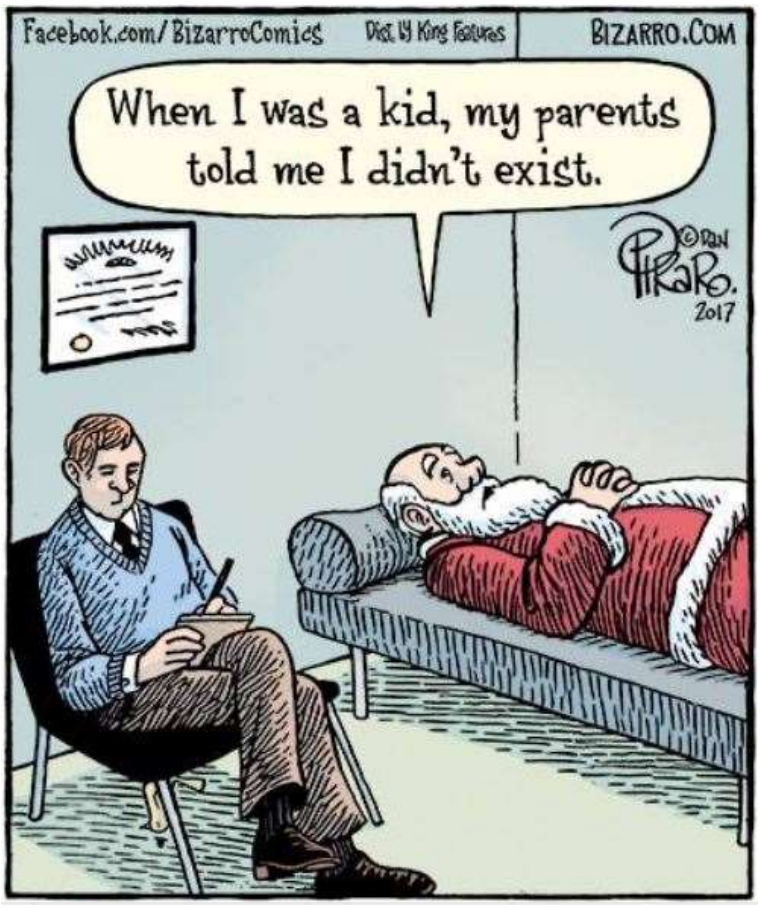
In the early days, Pierre Omidyar's Auction Web, the consumer-to-consumer marketplace, shared a domain with a page for Tufts University alumni and another full of information on ebola. Over the next three years, only one of those passions would prove to be a billion-dollar business, and by 1998, Auction Web rebranded as eBay. After surviving the first dotcom bubble burst, eBay continued growing into one of the internet's biggest e-commerce engines. It bought PayPal in 2002 and soon had stores such as QuikOrder offering to sell your stuff on eBay for a small fee. Whether it was a hard-to-find car part, a coveted Christmas gift, or a half-eaten plate of French toast left behind by Justin Timberlake, eBay was the place to get it. Though eBay's presence has faded some, and it's currently struggling through a restructuring, its influence is evident today in some of the biggest online platforms.

There are two ways to write error-free programs; only the third one works.

Hotmail 1996

Hotmail (originally stylized as HoTMaiL as a riff on HTML) launched at a time when most people didn't use email and those who did accessed it at work or via clunky mailboxes tied to their ISP. That changed with the introduction of free, ad-supported webmail that could be opened through any browser. Hotmail wasn't the only company offering the service, but it quickly became the biggest, thanks to a viral marketing scheme that's become something of Silicon Valley legend. The trick was simple, every email sent from a Hotmail address would have a signature imploring the person reading to "Get your free e-mail at Hotmail." Within a year of launching, Hotmail had millions of subscribers, and in late 1997, Microsoft came calling.

Around the same time, Yahoo snatched up RocketMail and introduced its own free webmail client. Both Yahoo and Outlook (Microsoft's rechristening of Hotmail) remain popular email providers, but neither was able to keep pace with Google's Gmail, which arrived in 2004 and has ruled the category ever since.



Google **1998**

The idea that became Google owes a debt to academic publishing, where frequent citations are the surest sign of a paper's importance. Larry Page applied the same logic to webpages for his Stanford dissertation and with the help of his math whiz friend Sergey Brin, invented a product that consistently bested the most popular search engines of the day. Originally called BackRub, the search engine was renamed Google in 1996. Two years later, it was winning converts from the cluttered portals that ruled the day. Google the company grew into a behemoth of online advertising, cloud computing, and wind turbines, but Google.com hasn't changed all that much. The stark, white homepage, designed so simply because Brin didn't know HTML, was so out of place among the flashing word art and dancing babies of the late '90s that some users sat staring at it, waiting for the rest of the page to load before trying to search. Now, with 63,000 searches a second, Google doesn't have that problem.

Wikipedia **2001**

The Wikipedia page for “Democratization of knowledge” mentions two key engines that have driven “the acquisition and spread of knowledge amongst the common people.” There’s the printing press and there’s Wikipedia. Nearly two decades after it went live, the site isn’t overselling its own importance, even if it’s still working toward its stated goal to “compile the sum of all human knowledge.” Wikipedia now hosts well over 10 million articles in hundreds of different languages, all of them written and edited by volunteers. With growth has come respect. A decade ago, Wikipedia wasn’t considered anywhere close to a reliable source, but that has begun to change. Like any website, Wikipedia has seen its share of abuse and vandalism, but the site remains remarkably resilient, maintaining its core mission without preying on consumers in the way so many of its peers on this list have.

Helvetica and Times New Roman walk into a bar.
“Get out of here!” shouts the bartender. “We don’t serve your type.”

The Pirate Bay **2003**

What Amazon did for books, the Pirate Bay has done for music, movies, software and, in their electronic format, books. The key difference? On the Pirate Bay, long the web’s leading index of torrents, everything is free, because it’s pirated. Launched by a Swedish anti-copyright group in 2003, the Pirate Bay has been the target of endless legal challenges for allowing users to download copyrighted content. In 2009, the three men behind the site were sentenced to a year in prison and $3.5 million in fines. But that wasn’t enough to kill the Pirate Bay—nothing has been. As other torrent sites have folded, the Pirate Bay has attracted more users and managed to stay online, save the occasional hiccup. Now, after years of declining popularity in the face of easily accessible streaming options, torrents are making a comeback. And the Pirate Bay is still standing.

(**What is a torrent**? Most likely, you’ve heard of a torrent, used a torrent, or at least seen that term on the internet somewhere and whether you have actually used them or not, a lot of people don’t know what it actually is. When you hear the word “torrent” in the tech world, it usually refers to a computer file that contains data telling you where to find the information for which you are looking, the torrent file does not contain that actual information, for that you need a BitTorrent program such as uTorrent. The torrent file tells uTorrent where to go and look for and get the information.

For instance, let’s say you wanted to download a movie, you’d google the name of the movie and up would come several sites where you could download that movie for a price but it could also show you the movie as a torrent file. The torrent file does not contain the movie but it will show you one or more sites where other people have already download the movie and who are willing to share it with you. So, if you said “that will do me”, the torrent file tells uTorrent to copy that

movie from those other people's sites. There are two advantages here, one is obvious, you get it for free, and secondly, as you're downloading it from multiple sites, it comes down much quicker.

This is of course frowned upon in many countries and some have been prohibiting illegal torrents by blocking them, but as soon as they block one, up pops another.

In short, a torrent file acts as the key to find and start the downloading of the actual content. When someone is interested in receiving a shared file (i.e. books, music, video, documents, etc.), they must first obtain the corresponding torrent file by using a program such as The Pirate Bay above.

The sites from which you actually download the file are called "seeders," you as a downloader are called a "leecher".

A torrent download can be done in fragments, so in reality you're actually downloading bits of pieces of the full content from various sites which are later reassembled when all of the pieces are received.)

Facebook 2004

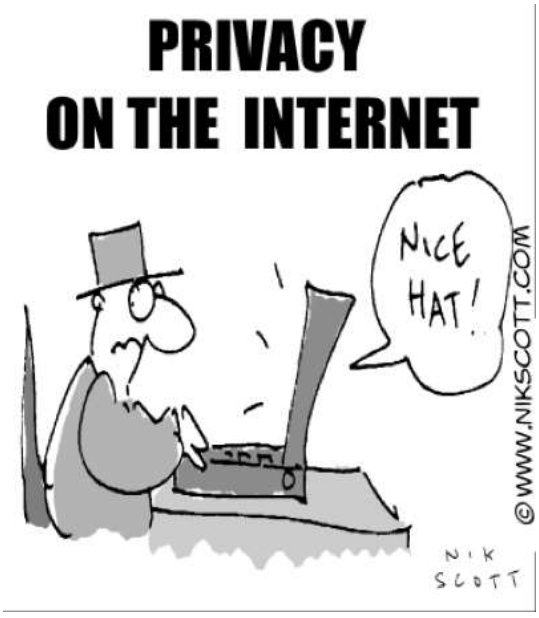
Facebook has come a very long way since it was thefacebook.com and only allowed Ivy League students to sign up. Mark Zuckerberg's site, inspired by the iconic HOTorNOT, is now one of the most valuable companies in the world. The enormous social network, boasting more than a billion active users, has done both good and bad. On one hand, it's allowed distant relatives to keep up

across time zones. On the other, it's turned our lives into easily packaged commodities for advertisers to slurp up and disrupted democracy as we know it. But hey, poking is still fun!

YouTube 2005

It's only 19 seconds long and nothing even happens, but "Me at the Zoo" is undoubtedly one of the most important internet videos of all time. The clip was the first video ever uploaded to YouTube, a site created either to share videos of a dinner party or to make it easier to find clips of Janet Jackson's infamous Super Bowl "wardrobe malfunction." What we all can agree on is that the site went live in May of 2005 and rocketed to success. A year and a half later, Google bought YouTube for $1.65 billion in stock and it quickly became one of the most essential, highly trafficked websites on the internet. YouTube has made careers, destroyed lives, and it shows no sign of slowing. As of last October, YouTube accounted for nearly an eighth of all internet traffic, trailing only Netflix.

THIS is the first ever YouTube clip



Twitter 2006

Twitter's first big moment came at South by Southwest in 2007, where the fledgling microblogging site was voted "Best of the Web" While some criticized the inherent triviality of tweets, others understood that that was the point. Widespread adoption soon followed and in 2009, Ashton Kutcher wrote in Time that the creation of Twitter is "as significant and paradigm-shifting as the invention of Morse code, the telephone, radio, television, or the personal computer." It might have

been an oversell, but not by much. A decade after it exploded, Twitter has aided revolutions, helped empower authoritarians, and created some very weird celebrities.

Wikileaks 2006

The trove of confidential U.S. military documents that WikiLeaks published in 2010 wasn't the whistleblower site's firs- time releasing information that world powers preferred to stay secret, but it was the one that brought WikiLeaks, launched with a mission of furthering "transparency in government," into the mainstream. It also turned its founder, Julian Assange, into a Pam Anderson-dating celebrity. Six years later, the site would hit the headlines once again when it published hacked emails from the Democratic National Committee. The slow, methodical rollout of the emails gripped the news media in the leadup to the 2016 election and led to accusations that Assange was trying to help Donald Trump, who claimed during the election, "I love WikiLeaks." Since then, the site has been in the news more for its founder's legal troubles than anything it's published. It might have had its day.

Pornhub 2007

There isn't much mystery to the success of Pornhub, which launched in 2007 on the radical idea that people on the internet wanted to see naked people. Three years later, MindGeek, the Canadian firm that owns many of the web's most popular porn sites, scooped up Pornhub and grew it into the largest hub of pornography on the web. They consume the third-largest amount of bandwidth, with only Google and Netflix ahead of them. (Who said sex doesn't sell?) Pornhub

has an enormous catalogue, some of it professional, some it amateur, much of it pirated, and proves Rule 34 of the internet ("There is porn of it. No exceptions.") all by itself. The site attracts 100 million visitors a day, but it still has detractors, and they're not all puritans. (See HERE)

GoFundMe 2010

Online crowd funding has seen a few major players in the last couple of decades, including Kiva, which allows users to give microloans to overseas entrepreneurs and Kickstarter which connects inventors (and con artists) with potential customers, but no crowdfunding platform is more symbolic of our time than GoFundMe, which was established as a way to ask friends to help pay for major life events. Turns out the most pressing major life events are medical emergencies and the bills that follow. Earlier this year, the company's CEO said a third of the money raised on the site goes toward medical expenses. GoFundMe users set up more than a quarter of a million medical fundraisers each year and raise more than $650 million as they compete in a dystopian (opposite of utopian) competition to see whose ailments are viral enough to allow them to avoid a life in medical debt.

A computer programmer's wife asks him to pick up some groceries on his way home from work. He asks what she needs and she says to pick up a litre of milk and if they have eggs, get a dozen. When he returns home, his wife asks why he brought home 12 litres of milk and he replies that they did indeed have eggs.

Reasons the F-35 is nearly unstoppable in the sky.

The triumph of the F-35 is obscured by the way in which news is reported. Program coverage often highlights the latest development, good but more often bad, without capturing the steady progress made over 16 years since the development contract was first awarded, nor the high priority that three U.S. military services have continuously assigned the program through multiple presidencies. What follows is a concise review of the areas of accomplishment that collectively demonstrate the F-35 program has become a smashing success.

All those arm-chair no-alls who blasted the F-35 have now gone silent and the winner is the F-35. Apart from the US, very smart people from Australia, Denmark, Italy, Netherlands, Norway, Turkey and the UK as well as from Israel, Japan and South Korea have all decided that the F-35 is the best aircraft.

A performance by the F-35 at the 2017 Paris Air Show was a turning point for the world's most advanced multi-role fighter, demonstrating that even when fully loaded with combat gear, it can out-perform the tactical aircraft of every other country. Although prime contractor Lockheed Martin has always professed confidence the F-35 would prove itself, a dwindling collection of critics, the flat-earth mob, continued to attack the plane citing outdated or simply erroneous arguments.

Those idiots fail to grasp that F-35 is one of the greatest technological achievements of this generation, a program that will assure global air dominance for the U.S. and its allies through mid-century. It also will help assure that aerospace remains America's most dynamic export sector. F-35 will generate tens of billions of dollars in trade earnings and tens of thousands of jobs, from over a dozen foreign customers. The plane has never lost a competition in which it went head-to-head with other fighters.

Testing. In 2017 the F-35 program wrapped up the most comprehensive flight test program in aviation history. The three variants of the fighter being built for the Air Force, Navy and Marine Corps have undergone 8,000 flights to gauge their performance without identifying a single show-stopper. Each of the variants has met all its "signature" specifications for stealthiness, making F-35 by far the most survivable fighter being built anywhere. Sensor fusion, networked operations, and other features have been thoroughly tested and retested, assuring the planes will always see first and fire first in aerial engagements. Tests of the Navy version were the most successful at-sea trials the service has ever conducted.

Operations. The Marine Corps version of the F-35 has been operational for two years and the Air Force version for one year. F-35s have deployed to Japan (from which they recently engaged in exercises with South Korea's military) and Europe (where they participated in exercises across the continent). Israel, the only Middle Eastern country approved to buy F-35, is also operating the plane. Over 200 F-35s have been delivered, with the number expected to rise to 600 in 2020. Over 400 pilots and 4,000 maintainers have been trained at 12 operating bases. In recent Red Flag exercises, the Air Force variant achieved a kill ratio of better than 20-to-1 against adversary aircraft while being available over 90% of the time.

Cost. The Air Force version of F-35, the one being bought by most allies, costs $85 million in 2019. That's about what the latest version of legacy fighters like the F-16 cost, equivalent to roughly ten minutes of US federal spending at current rates. It is also less than what a 737 MAX, Boeing's smallest next-generation jetliner, lists for. The peak year for F-35 production is scheduled in 2026, at which point all the fighters for all three domestic military services will cost less than a single day's worth of US federal spending ($13.6 billion versus $17.5 billion). If current trends hold up, the planes could be even cheaper: the price-tag for the Air Force version of F-35 fell 12% over the last two production lots.

Demand. Washington has not wavered from its plan to buy 2,457 F-35s since development began in 2001. Obviously, that would not be the case if the program had encountered major problems. It is unusual for three services to stick with a plan through multiple presidencies covering 16 years. Equally striking, almost all of the original international partners have stuck with the program, and several new players have signed on -- Denmark, Israel, Japan and South Korea. Canada is the only country that has wavered and in all likelihood, it will return to the fold once it sees the advantages of buying a highly survivable fighter operated by most of its key allies. F-35 has emerged as the global gold standard of next-gen air power.

Pilots. The most telling testimonials to F-35 excellence come from the pilots who have flown the plane. The Navy reported after the first at-sea trials of the carrier version that "the aircraft demonstrated exceptional performance throughout its initial sea trials." More recently, a squadron commander who participated in last year's Northern Lightning exercise in the US told an in-house Air Force publication, "I couldn't ask for anything better. It's like fighting somebody with their hands tied behind their backs." Another pilot flying adversary aircraft in the exercise remarked, "We just can't see them like they can see us. It can feel like you are out there with a blindfold on." Pilots generally say F-35 is far superior to legacy fighters.

Other nations might have aircraft that have a stronger punch, a longer reach and superior situational awareness but whatever the other fellow's training might be, if he can't see his rival to land a punch he's down before the first round is over. That's what makes the F-35 a game-changing aircraft, the one plane that can keep enemies at bay for another generation. It isn't just the best air power option Australia has.

See HERE

On board rubbish – what do you do with it?

Naval ships generate a lot of rubbish, aircraft carriers, which carry a lot of people and a lot of aircraft generate a huge amount. But what do you do with it?

The new HMS Prince of Wales carrier of the Royal Navy is trialling a new system that if works, will probably become the norm. Extreme heat from a burner reaching temperatures of more than

1,000C breaks down the material generated by the 1,000 people on board. This includes food, sewage and excess oils which contribute to a total of upwards of nine tonnes every day. The system is called Pyrolysis

The waste (“gash” in RN parlance) is converted into fuel, which then sustains the plants, meaning the burner can be switched off. One of the junior sailors responsible for the plants' operations, said: "The plants’ waste reduction ratio will benefit the ship’s company with us having far less waste to dispose of during 'out all gash' – and enable us to store the waste far easier."

The Pyrolysis plant can dispose of most waste at the rate of 150kg per hour, but not metals or glass which is crushed. Prior to the installation of the plant, rubbish was manually stored in metal drums and unloaded whenever the ship was serviced.

The system is switched on with the initial flame coming from burning fuel, but once underway, the fuel source is switched off and the rubbish itself is its own fuel. 150kg of waste becomes 1½kg of grey-blackish ash, which is easily stored until the ship is serviced.

How much does it cost to fuel an airliner?

Have a look at THIS.

And at last – the Apple gun.

See HERE

The history of Spam?

The history of spam started in 1864, over a hundred years before the Internet, with a telegram sent en masse to a number of British politicians. In a prophetic sign of things to come, the telegram was an advertisement for teeth whitening.

The first example of an unsolicited email dates back to 1978 and the precursor to the Internet, ARPANET. This proto-Internet spam was an advertisement for a new model of computer from Digital Equipment Corporation. It worked, people bought the computers.

By the 1980s, people came together on regional online communities, called bulletin boards (BBSs), run by hobbyists on their home servers. On a typical BBS, users were able to share files, post notices, and exchange messages. During heated online exchanges, users would type the word “spam” over and over again to drown each other out. This was done in reference to a Monty Python sketch from 1970 in which a husband and wife eating at a working-class café find that almost everything on the menu contains Spam. As the wife argues with the waitress over the preponderance of Spam on the menu, a chorus of Vikings drowns out the conversation with a song about Spam.

The use of the word “spam” in this context, i.e. loud annoying messaging, caught on, to the chagrin of Hormel Foods, the maker of Spam.

O

Over on Usenet, a precursor to the Internet that functions much like today's Internet forums, "spam" was used to refer to excessive multiple posting across multiple forums and threads. The earliest Usenet spam included a fundamentalist religious tract, a political rant about the Armenian Genocide, and an advertisement for green card legal services.

Spam didn't start in earnest until the rise of the Internet and instant email communication in the early 90s. Spam reached epidemic proportions with hundreds of billions of spam emails overwhelming our inboxes. In 1999, Melissa, the first virus that spread via macro-enabled Word documents attached to emails was let loose upon the digital world. It spread by ransacking victims' contact lists and spamming itself to everyone the victim knew. In the end, Melissa caused $80 million in damages, according to the FBI. Without any anti-spam legislation in place, professional spammers rose to prominence, including the self-proclaimed "Spam King" Sanford Wallace. True to his nickname, Wallace was at one time the biggest sender of spam emails and social media spam on sites like Myspace and Facebook.

It wasn't until the early 2000s that governments around the world started to get serious about regulating spam. Notably, all member countries of the European Union and the United Kingdom have laws in place that restrict spam. Likewise, in 2003 the United States put a set of laws in place cheekily called the CAN-SPAM Act (once again, Hormel just can't get a break). These laws, in the US and abroad, place restrictions on the content, sending behaviour and unsubscribe compliance of all email.

At the same time, top email providers Microsoft and Google worked hard to improve spam filtering technology. Bill Gates famously predicted spam would disappear by 2006. Under these laws a rogue's gallery of spammers, including the Spam King, were arrested, prosecuted and jailed for foisting penny stocks, fake watches and questionable drugs on us. In 2016 Sanford Wallace was convicted, sentenced to 30 months in prison, and ordered to pay hundreds of thousands in restitution for sending millions of spam messages on Facebook.

And yet spam is still with us. Sorry, Bill.

In spite of the best efforts of legislators, law enforcement and technology companies, we're still fighting the scourge of unwanted, malicious email and other digital communication. The fact of the matter is that the business of spam requires little effort on behalf of spammers, few spammers actually go to jail, and there's lots of money to be made. In a joint study on spam between University of California, Berkeley, and University of California, San Diego, researchers observed a zombie botnet in action and found the operators of the botnet sent out 350 million emails over the course of a month. Out of these hundreds of millions of emails the spammers netted 28 sales. That's a conversion rate of .00001 percent. That being said, if the spammers continued to send out spam at that rate, they would pull in 3.5 million dollars in the span of a year.

So, what, exactly, are the types of spam that continue to fill our inboxes to the brim and what can we do about it?

What are the types of spam?

There are several types of spam to consider. On one end of the spam spectrum, you have mostly benign marketing spam from unscrupulous sellers haranguing us with dubious get-rich-quick schemes, and various pills that haven't been approved by anybody. On the other end of the spam spectrum, you have the serious threats, cybercriminals attempting to break into your online accounts, steal your data, steal your money and spread malware. While marketing spam is annoying, it's not a significant threat. Emails of this type are mostly filtered out by your email software and whatever makes it past the filters is easy enough to identify as spam and flag for removal.

The latter group of threats is harder to combat and far more dangerous.

Advance-fee scams

First in our lineup of email threats are advance-fee scams. Also known as the Nigerian scam or 419 scam, because the scam originated in Nigeria (419 refers to the section of the Nigerian criminal code the scams violate). Despite lending its name to the infamous scam, only a small fraction of spam originates from Nigeria. The country ranks number 68 in top spam senders. The advance-fee scam involves a mysterious sender offering you a vast reward in exchange for a cash advance, usually as some sort of processing fee, required to unlock the larger sum. Once you wire the cash to the cybercriminal, the sender disappears with your money. There never was a princely fortune or secret inheritance to begin with.

Another variant of the advance-fee scam turns unsuspecting victims into money mules. Often described by scammers as "payroll management" jobs, victims' bank accounts are used to launder and transfer dirty money. In exchange, victims get to keep a portion of the ill-gotten gains for acting as the middleman. When the police come knocking, it's usually on the door of the unfortunate middleman as the criminal masterminds are nowhere to be found.

Scams like these seem fairly transparent, yet people fall for them every day due in large part to the deep bag of tricks scammers have at their disposal. These tricks are called social engineering. Social engineering refers to the methods scammers use to pressure victims into taking some sort of action. Social engineering often involves psychological manipulation, playing to the victim's greed, vanity, or empathy.

Phishing emails

Malwarebytes Labs, says of phishing emails: "Phishing is the simplest kind of cyberattack and, at the same time, the most dangerous and effective. That is because it attacks the most vulnerable and powerful computer on the planet: the human mind." Phishing emails trick victims into giving up sensitive information, e.g. website logins, and credit card info, by way of social

engineering and email spoofing. Spoofed emails mimic, or spoof, an email from a legitimate sender, demanding some sort of action. Well executed spoofs will contain familiar branding and content, and sound urgent, even threatening. Common phishing ploys include:

- A request for payment of an outstanding invoice.
- A request to reset your password or verify your account.
- Verification of purchases you never made.
- A request for updated billing information.

By tricking us into giving up valuable information, cybercriminals are able to hack the online services we use every day without any real technological savvy. To put it another way, why pick the lock when you can just steal the key?

Malspam

Malspam is any kind of malware spread via spam. Much like advance-fee and phishing emails, malspam relies on social engineering to trick recipients into taking some kind of action, often against our better judgment, like clicking a download link, or opening an attachment contained in the email that infects your computer with malware. In either case, these downloads and attachments often come in the form of Word, Powerpoint or PDF files with malicious code hidden in the scripts/macros (i.e. automated tasks). When the document is opened the scripts run, retrieving the malware payload from the command and control (C&C) servers run by the cybercriminals.

Malware payloads vary greatly. The malware payload may enslave your computer into a botnet for the purposes of sending out more spam. More often than not the payload will be a Trojan. The majority of malware attacks in 2018 for both businesses and consumers were identified as Trojans of some kind. Banking Trojans, for example, are designed to steal sensitive financial information off your computer and in an interesting twist, some Trojans, e.g. Emotet and TrickBot, are now being used as a delivery mechanism for other malware, like ransomware, adware, spyware, or cryptojackers.

Spam on mobile/Android

Have you ever received a robocall? That's call spam. What about a text message from an unknown sender attempting to sell something, maybe even containing a link to who knows what? That's text message spam. Welcome to the hellacious world of mobile spam.

Now that mobile devices are commonplace, and Internet calling (VOIP) is cheap, spammers have a whole new way to spew out unwanted communication. The Android userbase alone includes more than 2 billion users for cybercriminals to target. The most common mobile phone scams, as reported by USA Today, are pre-recorded scam messages purportedly from banks, credit card companies, cable companies, and debt collectors. Another robocall scam targeting the immigrants involves a pre-recorded message

claiming to be from the appropriate consulate, telling the recipient there's an important document for them. Naturally, retrieving the document costs money.

Unless coming from a charity, political campaign, healthcare provider or purely informational call from a business or service you use, robocalls are illegal. Ditto for text messages. (See HERE)

How can I stop spam?

Now that you're informed about spam, here are some tips on how to identify phishing emails and malspam and prevent yourself from becoming a victim.

Don't respond to spam. Our first tip for stopping spam is: stop responding to spam. Have you ever read a comically bad spam email and wondered "Who actually clicks or responds to these things?" Well, wonder no more. In a spam survey conducted by the Messaging, Malware and Mobile Anti-Abuse Working Group, 46% of respondents said they clicked or replied to spam out of curiosity, to unsubscribe, or to learn more about the products/services being offered. Don't be one of these people. By responding to spam you demonstrate to spammers that your email is valid and they will send you more spam.

The same advice applies to mobile phone spam. Just hang up. By pressing "one" to opt-out or engaging with scammers in any way, you're demonstrating that your phone number is valid and that you will respond. Moreover, by speaking, scammers can record your voice and use audio samples of you saying "yes" to authorize charges for things and services you don't want.

Turn your spam filter on. The email providers do the hard work when it comes to stopping spam. Most bulk email never even makes it past our email filters and into our inbox. Granted, legitimate emails sometimes make their way, erroneously, into the spam folder, but you can prevent this from happening in the future by flagging these emails as "not spam," and adding legitimate senders to your contacts list.

Turn macros off. Definitely don't enable macros by default and if someone emails you an attachment and the document asks you to "enable macros," click "no," especially if you don't know the sender. If you suspect it may be a legitimate attachment, double check with the sender, and confirm that they, indeed, sent you the file.

Learn how to spot phishing emails. Here are the five red flags for spotting a phishing email. If you see any of these, then you're probably looking at a phishing email.

The sender's address isn't correct. If it's a legitimate email the sender's address should match the domain for the company they claim to represent. In other words, emails from PayPal always come from example@paypal.com and emails from Microsoft always come from example@microsoft.com.

The sender doesn't seem to actually know who you are. Legitimate emails from companies and people you know will be addressed to you by name. Phishing emails often use generic salutations like "customer" or "friend."

Embedded links have unusual URLs. Vet the URL before clicking by hovering over it with your cursor. If the link looks suspicious, navigate to the website directly via your browser. Same for any call-to-action buttons. Hover over them with your mouse before clicking. If you're on a mobile device, navigate to the site directly or via the dedicated app. Text message spam often includes links to spoofed sites designed to capture your login.

Typos, bad grammar, and unusual syntax. Does it look like the email was translated back and forth through Google Translate several times? It probably was.

The email is too good to be true. Advance-fee scams work because they offer a huge reward in exchange for very little work. But if you take some time to actually think about the email, the content is beyond reason.

There are attachments. In the world of email communication and marketing, attachments are a big no-no, and businesses generally don't send emails with attachments. You can read more about phishing emails and how to spot them on the Malwarebytes Labs blog.

Use multi-factor authentication. With two-factor or multi-factor authentication, even if your username and password are compromised via a phishing attack, cybercriminals won't be able to get around the additional authentication requirements tied to your account. Additional authentication factors include secret questions or verification codes sent to your phone via text message.

Install cybersecurity. In the event that you click a bad link or download malware sent to you via spam, good cybersecurity software will recognize the malware and shut it down before it can do any damage to your system or network. With products for home and business, Malwarebytes has got you covered wherever technology takes you. Not to mention threat protection on the go, Malwarebytes for iOS blocks all unwanted calls and text messages and if you click a malicious link in a spam text, Malwarebytes will stop the bad site from loading.

Side note for Mac users—don't go thinking you can click links and open attachments with impunity. You too can be a victim of malware. Malwarebytes for Mac protects you from the growing threat of Mac malware.

T