



Bind the Nation together through the correspondence of the people...digitally

How to expand the U.S. Postal Service's legacy of trust to electronic communications

Introduction

Although nearly 100% of Internet users in the United States use email, many citizens are still reluctant to trust it for their most valuable communications. While electronic messaging provides a fast and convenient way to communicate, fraud, identity theft, and privacy violations run rampant across the Internet—limiting the potential value of the medium. A recent development combats these challenges to electronic correspondence.

“The Postal Service shall have as its basic function the obligation to provide postal services to bind the Nation together through the personal, educational, literary, and business correspondence of the people.”

U.S.C. Title 39 § 101(a)

For over 200 years the United States Postal Service (USPS) has provided a reliable means for corresponding and protected our most important communications. Whether you're sending a personal note or a highly sensitive or valuable item the US Mail has always maintained a legacy of trust. At the birth of the United States, the nation's founders realized that in order to unify a new nation, correspondence must be reliable and trustworthy. The service has evolved from its inception as a series of surveyed and protected roads by adopting and adapting to new technologies to become the world's most expansive and sophisticated logistics system. Today the Postal Service is taking the next step to fulfill its obligation "...to bind the Nation together through the correspondence of the people..." by expanding its reputation for reliability and protection to cover electronic communications.

Mail, Email and the Internet

In the 1990's the Internet was on its way to delivering its vision of a truly connected and digital society. Among other market segments, two seemed particularly suited to advance to the online age: email and banking.

Email has been around longer than the Internet, but with the advent of the Internet, email was a natural fit for a global network. Messages and electronic documents could be sent and received instantly, anywhere in the world. Users readily envisioned a future where email and paper mail were essentially the same—without having to wait for the physical item to be delivered. Email though has remained an analogy to—not an extension of—physical mail.

www.epostmarks.com

epostmarks, inc. 45 Exchange Blvd, Suite 1100 | Rochester, New York 14614 | 585.546.4410



Online banking was another analogy that seemed destined to replace its brick-and-mortar cousin. The difference between the progress of email and online banking was that online banking was truly an extension of traditional banking. It was offered by the same institutions and the money in the account was the same whether it was accessed at a computer over the Internet or in a bank branch. However, without a true extension of physical mail to communicate with their customers, the banking industry was forced to create new constructs.

Online banking portals: a virtual experience

Portals were defined by Gartner in 2000 as “a window into the information of the Internet” saw an explosion in popularity. Information architects began employing a model reflecting a one-stop user interface within the context of a web page. Banks employed this model—offering typical branch services through an online control panel that allowed users to perform typical banking activities such as transferring funds, viewing balances, paying bills, and other services¹.

These portals allowed financial institutions to provide a virtual banking experience, and gave the users a more convenient and fast electronic version of visiting a branch to conduct business. However, when it came to sending necessary correspondence like statements, notices, and other private data, banks still used paper mail because of the privacy and security concerns related to a communication medium that lacked any standards, rules, or enforceability. When they do choose to use email, financial institutions send an email message indicating that the customer should visit the portal to access the information. This notice generally includes a link back to the portal for convenience to the user.

Rise of phishing and email fraud

The Internet email system has had no reliable method of creating trust from end-to-end. Without the oversight of a universally trusted authority, reliably confirming who is actually sending a particular message is virtually impossible. The existence of this flaw, combined with the near-universal adoption of financial institutions using emails containing links encouraged the development of email fraud in two ways.

- 1) Sending notification messages with in-line links trained customers to expect links from their financial institutions. This training didn't have disclaimers that the email system isn't as trustworthy as paper mail. While most knew that there was no Postal Service to protect them in the electronic world, they didn't consider that a fake message could come from anywhere and links could lead anywhere, including fake websites.
- 2) It is easy to create fake messages with links to fake websites that look like the real thing.

¹ Shaw, R. (2000). *Portals: An Introduction*. Gartner Group, Inc.





In retrospect, it seems obvious that criminals would exploit this weakness in the communications infrastructure. Not establishing end-to-end trust in the beginning gave way to one of the fastest growing and farthest reaching fraud schemes in history: “Phishing”.

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card details, etc. by masquerading as a trustworthy entity in an electronic communication. These trustworthy entities are often financial institutions that experience multi-faceted cost implications from this insidious type of fraud. Most obviously there are direct monetary losses. Additionally, the cost to the brand of the phished institution can be just as costly as the direct financial damages.

Phishing has grown over the past few years to attack over 2,000 brands across 30 countries. Projected to cost the U.S. economy \$8.4 billion in 2009, up almost 100% from 2007, phishing is having a devastating impact on email communications². These costs do not only impact the financial institutions. Estimated non-monetary cost to victims is \$1.8 billion, with roughly 15% of cases incurring non-monetary losses including:

- Denied credit or other financial service;
- lost time to resolve problems;
- debt collector or creditor harassment;
- criminal investigation, arrest, and conviction;
- civil suits filed or judgment entered;
- denied employment or job loss³.

Online compliance

The banks’ use of portal notification messages with links created an unforeseen opportunity for criminal activity. Sending messages this way also had an impact on compliance. Financial institutions represent some of the most regulated organizations in the nation. When dealing with money, consequences are high. Financial institutions have serious responsibility to ensure that customers receive the highest degree of care.

One particularly important aspect of compliance revolves around required communications. Consider monthly statements in both the physical and banking portal models. Providing bills and statements are a required aspect of banking and other financial relationships. In the physical world, a statement is enclosed in an envelope and sent through the mail. This private and trusted communication is sent through a

² The Cost of Phishing: Understanding the Trust Cost Dynamics of Phishing Attacks. Cyveillance December, 2008

³ Identity Theft Cost and Prevalence. Government Accountability Office 2002





technology model protected by the Postal Service and provides the recipient the information required. In the electronic world of banking portals, a link is sent to the recipient who must then return to the financial institution to collect the private information. Since no information is actually sent, the compliance requirements are not fully met until the recipient returns to the portal to collect it.

In addition to the fear of phishing, notification links are one of the primary reasons that paper turn-off rates for the average financial institution is no higher than 15%⁴ despite modest eStatement and eBilling adoption rates. When paper turn-off does occur, financial institutions are often forced to begin sending paper when the customer fails to regularly log into the portal to “download” or view the communication. This simple failing of banking portal notifications leave financial institutions lacking the compliance necessary to effectively migrate away from paper.

Solution

USPS history of protecting communications

The authors of the Constitution had such a strong belief in the importance of the Postal Service that they provided specific provisions to establish it in Article I. Before establishing Federal courts, allowing for the declaration of war, and raising an army or navy was the directive to create post offices.

Since its inception, the U.S. Postal Service has protected the correspondence of the people pioneering into new frontiers as our nation evolved. In the 19th century during a period of rapid growth, the Postal Service was the communications system that helped bind the nation together. They developed new services that have lasted into the 21st century and embraced new technologies subsidizing the development of every major form of transportation. They made decisions to fund post routes that supported national development and instituted services to benefit all residents of the country.

The U.S. Postal Service has a long legacy of trust, beginning in 1792 when postal officials were prohibited from opening the mail. That legacy has grown to include an extensive national and international network and it continues today with USPS maintaining the status of most trusted federal agency and third most trusted brand in the United States.

The U.S. Postal Service recognizes that people have changed the way they communicate. Digital communications require the same prompt, reliable and efficient services as the brick and mortar world. Crime has infected the email system and the nation requires a trust model it can rely upon to help fix it.

⁴ The Greening of America: One eStatement at a Time—Forrester, 2008





How this applies to email

The Internet represents the newest frontier we are conquering and its development follows many of the same patterns seen when settling the western frontier. The frontier brought speculators and land-jobbers, buying up land, often in whole counties at a time. Then came the restless pioneer, who built his log cabin, cut the trees, sowed a handful of grain, and then gave way to the impatient longing that possessed him, and moved on. This made way for a second line of settlers, with some money, who purchased the previous settlers' improvements and availed themselves of the results of their labor. These in their turn moved on, leaving the country more habitable behind them. Next came the permanent settlers, the founders of towns and villages, and civilization began to settle upon the land⁵.

At the beginning of the Internet, speculators drove the dot-com bubble. Since the bubble burst, the restless pioneers and the second line of settlers have been investing and building value into the system. Many have availed themselves of the results of others' labor, leaving an increasingly more habitable territory behind. We now see many web properties that provide true value and hold the promise of even more.

Many unsettled areas of the internet that require the absolute autonomy needed to attract the pioneering spirit still remain. For those who desire a more stable existence, it is necessary to create a trusted framework of rules accepted by those who participate. The U.S. Postal Service, most trusted by the nation, has the ability to establish and implement such a framework for email and other online communications. It falls directly within the realm of expertise they have been honing for over two and a quarter centuries: binding the nation together through the correspondence of the people.

When crimes are committed, the USPS creates a clearer path for enforcement. The U.S. Postal Inspection Service, one of our country's oldest Federal law enforcement agencies has a long, proud, and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public. This organization has been given direct authority from the Department of Justice to enforce:

- Criminal conduct in which the Postal Service is an actual or intended victim.
- Criminal conduct that directly affects electronic messages conveyed by the Postal Service and the counterfeiting or misuse of any electronic postmarks used by the Postal Service.
- Criminal conduct directed against any computer, computer system, communication system, delivery system, payment system or other similar property owned or leased by or provided to the Postal Service.

⁵ Bancroft, H. H. (1902). *The Great Republic by the Master Historians*





By establishing a trusted framework, the USPS will create an environment where society can progress to the next level electronically. Having a trusted third party participate in transactions creates a comfort factor, allowing higher value transactions to take place in a manner compliant with the laws and regulations that have established our nation.

Conclusion

The modern email system has evolved in such a way that fraud and other criminal activity negatively impact the medium's efficacy. Email lacks trust and as such cannot operate within the regulatory framework already established by our nation. Our history has seen similar evolutions from which we can draw critical lessons. In order for this new frontier of the Internet to truly establish itself as a cornerstone of our communications foundation it must become "civilized". The USPS has a long history of protecting the correspondence of the people. They are prepared to assist with the challenges facing this troubled medium and their help is desperately needed.

