The Threat of Political Phishing

C. Soghoian[1], O. Friedrichs[2] and M. Jakobsson[3]

[1]School of Informatics, Indiana University Bloomington, USA
[2]Symantec, Inc, USA
[3]Palo Alto Research Center, Inc, USA

Abstract

Internet based donations to political candidates are now a vital part of any successful campaign. Tens of millions of dollars are raised online each year, primarily in sub one-hundred dollar amounts from individuals around the country. Politicians have exempted their own campaign donation solicitation emails from federal anti-spam legislation, and their campaigns encourage risky behavior by teaching users that it is OK to click the "donate" button on an unsolicited email that arrives from a candidate. While not yet a major problem, fraudulent websites that masquerade as genuine campaign sites aiming to defraud donors are a significant threat on the not-so-distant horizon. These political phishing sites are easy to create, and extremely difficult for users to detect as not authentic. In this paper, we discuss threats against online campaign donation systems, and the unique factors which make this type of online commerce particularly vulnerable to fraud based attacks. We explore the threat that phishing attacks utilizing typo squatting and cousin domain names could pose to the 2008 presidential election. Finally, we propose a realistic and cost-effective solution to the problem.

Keywords

Phishing, Online Fraud, Internet Commerce.

1. The Importance of Online Campaign Donations

Over the past few years, online campaign donations have increasingly become a significant portion of the overall campaign fundraising process. Hillary Clinton's presidential campaign raised over eight million dollars online during the third quarter of 2007, more than one year before the 2008 presidential election (Stirland, 2007). Republican presidential candidate Ron Paul holds the single-day online contribution record, after raising four million dollars on the 5th of November, 2007 (Wolf & Parker, 2007). More than half of Democrats gave online in 2004; double the percentage of Republicans. Furthermore, over 80 percent of the contributions by people ages 18 to 34 were made over the Internet (Edsall, 2006).

Tens of millions of dollars of campaign donations are now raised annually through the Internet. This logically means that hundreds of thousands of consumers have shown a willingness to hand over their credit card numbers in response, in many cases, to unsolicited donation request email messages from the candidates. While this

is no doubt good for the politicians, this kind of behavior is very risky, and could easily be taken advantage of by phishers.

The very success of a campaign donation solicitation depends upon impulsive reactions by the potential donors. Millions of email messages are regularly sent off to possible benefactors, typically in response to some act committed by the opposing party. Donors are made to feel shocked, repulsed or alarmed and then urged to donate money in order to help to combat the evil of the day. This strategy is aimed at producing impulsive reactions on the part of the donor. From the perspective of the political campaigns, giving now is far preferable to giving later.

The problem with this approach is that unlike an impulsive purchase at Amazon.com, a political donation does not result in the sale of a physical good. Other than a thank-you email, the donor typically does not receive anything after submitting their donation. This means that it is very difficult for some to confirm after-the-fact who they donated to, or to learn that they may have been scammed. There have been some recent efforts to spread consumer awareness of security threats with user education (Srikwan & Jakobsson, 2007). However, in this paper we focus instead on more direct methods enabling campaign donation sites to safely establish user trust.

2. Domain Name Problems

American consumers each have, on average four credit cards (Experian, 2007). While customers may open and close cards over time, the names of the major banks typically stay the same (barring mergers and acquisitions). For those consumers who check their online bank and credit cards on a regular basis, it is quite possible for customers to memorize the website address of the bank sites that they login to regularly. More importantly, while banks overhaul the look and feel of their websites from time to time, the addresses stay the same. Citibank's website, www.citibank.com was located at the same address in 2003, 2005, 2007, and will most likely still be accessible at the same location in 2009. Banks spend significant sums of money in establishing well known and trusted brands. It is simply not in their best interest to change their name every few years.

Contrast this to the political system in the United States where candidate brand turnover can be very high. Candidates for particular public offices change on a regular basis, as successful politicians seek to advance their careers. Someone who solicits campaign donations for a House of Representatives run in 2004 may very well come back to solicit donations in 2006 as a potential Senator. Furthermore, for every politician who wins an election, there is typically at least one other opposing candidate who lost the very same race. The logical side effect of this is that even if a candidate successfully wins and retains the same office year after year, the opposing political party will typically replace the candidates that lost with someone else more likely to win.

While some political campaigns select Internet domain names that can be reused in the future, many others do not do so. Examples of this include domain names

associated with a specific political office,[1] and those tied to an election being held in a specific year.[2] In addition to having to print new bumper stickers in preparation for future elections, candidates also have to work to spread knowledge of their new domain name. The time and money spent on making the public aware of joesmith08.com will be wasted when Joe Smith runs for re-election in 2012. On top of all of these problems, it is often not possible for campaigns to purchase all of the alternative possible domain names for a candidate. Other individuals often snap up quite reasonably believable alternative domain names.

This leads to a state of confusion for the voter, where it is simply not possible to reasonably predict or confirm the location of the official website for a politician's campaign. Should a potential donor visit joinrudy08.com, or rudygiuliani.com, barack.com or barackobama.com, fredthompson.com or fred08.com? If a user clicks on a web advertisement that takes them to hillary08.com, how can they be sure that they are at her official campaign website? While some of the alternative domains are purchased by fans, others can be purchased by those who oppose the candidates. Examples of this include gwbush.com (Raney 1999) and whitehouse.com (Swartz 1998), both of which at one time or other, hosted content that the politicians they targeted certainly did not appreciate.

2.1. Typo and Cousin Domains

Typo squatting seeks to benefit from a mistake made by the user when entering a URL directly into their web browser's address bar. An errant keystroke can easily result in the user entering a domain name that differs from the one that they intended. Typo squatters seek to benefit from these common mistakes by registering domain names that correspond to common typos. Whereas in the past, users making typos were most likely to receive an error indicating that the site could not be found, today they are likely to be directed to a different web site. In many cases this site may host advertisements; however the potential for more sinister behavior also presents itself.

We conducted two tests in order to examine current domain name registration data for 17 of the main presidential candidates for the 2008 election. Firstly, we conducted a test in order to determine how widespread typo squatting was on each candidate's domain. Secondly, we examined domain name registration data in order to identify cousin domain names (Jakobsson, 2007). For our search, we define a cousin domain name as one that contains the candidate domain name in its entirety, with additional words either prefixed or appended to, the candidate domain name. In this context we would consider domain names such as presidentbarackobama.com or presidentmittromney.com as a cousin domain name from the candidates' core domain names of barackobama.com and mittromney.com respectively.

---

[1] Dennis Kucinich's www.dennis4president.com.

[2] Fred Thompson's www.fred08.com and Rudy Giuliani's www.joinrudy08.com.

Figure 1: A synthetic example of a political phishing email demonstrating the ease with which an attacker can falsify the header information and content to look as though the email came from a political party. While a legitimate email from the Democratic Party would come from democrats.org, this synthetic phishing email lists democratic-party.us as its source, a website that was registered by the authors of this chapter and is in not connected to the official Democratic Party. This example shows the power of cousin-domain attacks, and in particular, against political campaign websites.

For the purposes of our analysis, we consider a domain to be typo squatted if it has been registered in bad faith by someone other than the legitimate owner of the primary source domain name. We have visited those web sites for which typos currently exist and confirmed that they were in fact registered in bad faith. We have filtered out those that directed the visitor to the legitimate campaign web site as well as those owned by legitimate entities whose name happens to also match the typo domain.

We can draw two clear conclusions from the results of our analysis. Firstly, we can see that a large number of both typo and cousin domain names have been registered by entities other than the candidate's own campaign. In analyzing our results, we find that many of the registered web sites, both in the typo squatting case as well as the cousin domain name case are registered for the purpose of driving traffic to advertising web sites.

Secondly, we see that candidates have not done a good job at protecting themselves by proactively registering typo domains to eliminate potential abuse. In fact, we were only able to find one single typo web site that had been registered by a candidate's campaign - www.mittromny.com. All other typo domains were owned by other third parties that appeared unrelated to the candidate's campaign.

While advertising has been the primary motive behind the registration of typo and cousin name domains to date, the potential for more measurable damage using these techniques is highly probable.

Domain Name	Registered Typo Domains	Example	Registered Cousin Domains	Example
barackobama	52 out of 160	narackobama	337	notbarackobama
brownback	0 out of 134		152	runagainstbrownback
chrisdodd	14 out of 145	chrisdod	21	chrisdoddforpresident
cox2008	3 out of 92	fox2008	50	johncox2008
gilmoreforpresident	0 out of 276		20	jimgilmore2008
gohunter08	1 out of 150	ohunter08	23	stopduncanhunter
hillaryclinton	58 out of 191	hillaryclingon	566	blamehillaryclinton
joebiden	15 out of 125	jobiden	43	firejoebiden
johnedwards	34 out of 170	hohnedwards	190	goawayjohnedwards
johnmccain	20 out of 137	jhnmccain	173	nojohnmccain
joinrudy2008	9 out of 173	jionrudy2008	123	dontjoinrudy2008
mikehuckabee	3 out of 167	mikehukabee	28	whymikehuckabee
mittromney	18 out of 123	muttromney	170	donttrustmittromney
richardsonforpresident	2 out of 340	richardsonforpresiden	69	nobillrichardson
ronpaul2008	11 out of 143	ronpaul20008	276	whynotronpaul
teamtancredo	1 out of 170	teamtrancredo	16	whytomtancredo
tommy2008	1 out of 107	tommyt2008	30	notommythompson

Figure 2: Typo squatting and cousin domain analysis results. Many typo domain names were already registered and being used in bad faith. In addition, even more cousin domain names were registered, both in support of a candidate, and in many cases, to detract from a candidate. Note that all domains and examples are in the .com top level domain.

3. Political Phishing

Political phishing has been observed in the past, although only in a few instances. During the 2004 US presidential election, phishers targeted the Kerry-Edwards campaign (Seltzer, 2004); a campaign that was acknowledged as being at the forefront of leveraging the Internet for communications. At least two distinct types of

phishing were observed during that campaign. In one case, phishers set up a fictitious web site in order to solicit online campaign contributions shortly after the Democratic National Convention, stealing the victim's credit card number, among other information. In the second case, phishers asked recipients to call a for-fee 1-900 number, whereby the victim would subsequently be charged $1.99 per minute (Hermida, 2004).

We now explore attacks, both existing and potential, against the online fundraising process in which phishers create fake, yet believable campaign websites with realistic looking domain names. These websites would then be used to lure users into submitting their credit card numbers and other financial information. Were such phishing sites to become common, donors could lose confidence in the online political donation system and stop giving.

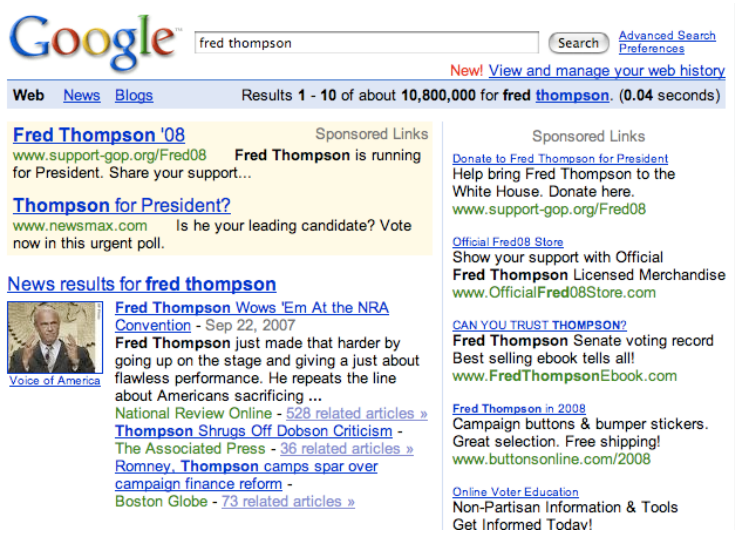

Figure 3: A synthetic example of an attack using text advertisements placed on a search engine to direct users to a political phishing website. This demonstrates the ease with which advertising networks can be used to lay the groundwork for more sophisticated attacks. The official website of the Republican Party is www.gop.org and Fred Thompson's 2008 Presidential campaign site is www.fred08.com. However, the text advertisements in this synthetic attack sent users to www.support-gop.org/Fred08, a domain name registered by the authors of this chapter. This further demonstrates the power of cousin-domain attacks.

3.1. Drawing Users In

The most obvious technique for drawing in potential phishing victims to a fake political campaign website is email. This is currently the dominant technique used in other phishing scams, and is ideal for political deceit. Many banks have spent

significant amounts of money and time trying to educate users against clicking on links and in responding to emails from anyone claiming to be their bank. The opposite is true for political candidates, who increasingly turn to email lists in order to reach potential voters, and depend on impulsive user reactions to trigger donations. The importance of unsolicited email messages to the political campaigns that send them can be inferred from the fact that Washington politicians made sure to exempt their own contribution requests from the CAN-SPAM Act, which bans most forms of unsolicited commercial email (McCullagh, 2003).

Phishers often have no way of knowing which bank a potential victim has accounts with. Thus, in cases where emails are indiscriminately sent out to millions of addresses, phishers will often masquerade as one of the major US banks (Citibank, Chase, Bank of America, etc). The logic behind this is simple: a random victim is more likely to be a customer of one of the large banks than a small regional financial firm. Pretending to be one of the financial market leaders will provide the phisher with highest rate of return on the resources he invests in his attack.

Political phishing does not suffer from the problem of hundreds of different banks, or even the five or six largest companies. There are only two mainstream political parties in the United States: The Democrats and Republicans. A phisher has at least a 50/50 chance of guessing the correct political party for a potential victim. By using more advanced user reconnaissance techniques such as invasive browser sniffing (Jakobsson & Stamm, 2006) or browser based timing attacks (Felten & Schneider, 2000) to learn which news and political websites a user visits, it might be possible to guess a victim's political affiliation with a higher rate of success.

3.2. Social phishing

While email is currently the dominant method of luring users to phishing sites, there are several other promising strategies. Users are particularly vulnerable to deceit based attacks when the phishers take advantage of knowledge of the victim's social group (Jagatic *et al.,* 2007).

Detailed records of political donations, including contributor name, city, state, zip code and principal place of business are published online by the Federal Election Commission. Through the use of online telephone books, social networking sites and personal home pages, it may be possible to link a donation record to an online identity and email address. This information, especially when combined with knowledge of a person's employer, could be used to execute highly targeted and accurate phishing attacks.

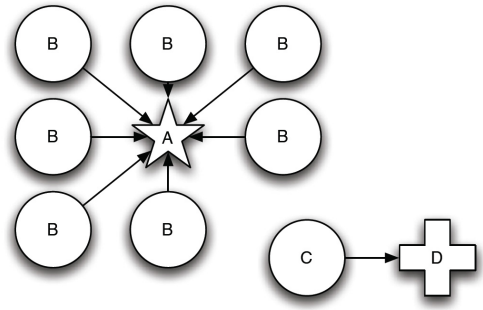

Figure 4: The figure depicts the currently used infrastructure for online campaign contributions, and an attack on the same. Potential donors are sent to the payment aggregator (A) by different campaign websites (B). At the same time, a malicious website (C) sends traffic to a malicious payment aggregator (D), which may be an spoofed version of A. The core of the problem is that the campaign websites often have a very low URL recognition among donors, those donors will make a security decision while on the supposed campaign website, and will therefore be vulnerable to attack by D.

3.3. Phishing via advertisements

Web-based advertisements, both those using graphics, text and more complicated flash-based content have been used to spread malware and trick users. One example of this is a September 2007 incident in which malicious flash advertisements were served millions of times on a number of high profile websites, all of which were serving ads placed by an advertising company owned by Yahoo (Goodin, 2007). In a previous incident, a malicious flash advertisement was able to infect over a million users of the popular social networking site MySpace users with a trojan (Krebs, 2006). Google's popular text-based advertising network has also been used to spread malware, although doing so did at least require that the user click on the ads (whereas the flash ads silently installed the malware without any user interaction). A report in April 2007 indicated that criminals were purchasing Google text for legitimate websites such as the Better Business Bureau. Users clicking on the ads would be taken to an intermediate website, which would attempt to silently install password-stealing malware, before then taking the user to the actual Better Business Bureau website (Krebs, 2007). Using one or more of these techniques, it should be possible for phishers to place advertisements for politics-related keywords (such as the names of the candidates), which would take unwitting users who click to a phishing site masquerading as a campaign donation website.

4. Website Authentication

The previous section listed three methods with which a phisher could draw traffic to a political phishing website. Section two explained why users simply cannot be expected to know which domain names are the authentic and official websites for the

politicians they are interested in. We now discuss why key anti-phishing technologies, including two-factor authentication, that have been widely deployed in the Internet banking market will not be able to protect political websites.

Consumers typically have ongoing relationships with their banks. This provides both entities, the bank and the consumer, with additional means with which to verify each other. Users who are tricked into providing their login details to a website masquerading as their bank may become wise to the fraud when the fake website does not display their valid account number, balance or recent transactions. Recent advances in two-factor authentication technology have also provided customers with methods to detect websites masquerading as their banks. Schemes such as Bank of America's SiteKey system provide a way for the bank's website to prove to the user that it is authentic. These authentication technologies can be bypassed with deceit augmented man-in-the-middle attacks (Soghoian, 2007), but this at least raises the bar for the attacker.

Many donors do not have an ongoing financial relationship with political candidates. This makes it very difficult for a candidate's website to prove its authenticity to the user, and consequently, provide few signals for users to detect when a site is not authentic. From the perspective of the user, if the site looks legitimate, it probably is.

The easiest way for an attacker to make a phishing page look authentic is to simply clone the content of the original website. Web cloning tools such as the ScrapBook extension (Murota Laboratory, 2006) for the Firefox web browser can be used by attackers to create a working local copy of a remote political campaign website, which the attacker can then modify, upload to a server, and make available online with a fake, but authentic-looking domain name.

As the attacker controls and can edit the local cloned copy of his new political phishing site, it is possible for her to enhance the original content in order to optimize it for phishing. One example of this would be to expand the payment options accepted by the website, as most political campaign websites only permit credit cards donations, to accept PayPal and electronic bank transfers.

5. Fixing the Political Phishing Problem

Earlier sections of this paper explained the factors which could make political phishing a major problem in the future: The large amounts of money being collected by political campaign sites, users giving their financial information to untrusted websites and the practical issues preventing users from being able to safely differentiate legitimate and fake political campaign websites. We now explore potential solutions to this problem.

Figure 5: A synthetic example of a legitimate political campaign donation website hosted by PayPal, and branded extensively with its logos. Were political phishing to become a major threat, a site similar to the one pictured would do much to encourage user trust in online political donations. The use of a strongly branded service, such as PayPal, as a starting point for donations has the benefit of increased URL recognition amongst users. It also benefits from the security features made possible with pre-established relationships between the user and the payment portal (such as PayPal's Security Key), and could leverage the financial service providers' existing anti-fraud measures that political candidates and their existing payment clearing houses may not have access to.

5.1. Consolidation at the back end

It simply does not make good business sense for each candidate to pay to re-invent the technology necessary for a campaign website. Most political candidates' websites share enough common features that code reuse makes far more sense. As a result, a small number of companies have been able to dominate the niche market of political campaign software, with one single company providing its software to more than two-thirds of the federal Democratic party political campaigns in 2004 and 2006 (National Geographical and Political Software, 2007). These companies provide turn-key solutions for candidates, permitting one or two tech staff members to install and deploy a sophisticated campaign website without too much work.

Thus, while a potential donor can visit one of the hundreds of different political candidates' campaign websites, most of the sites will be running the same back-end software that will be sending credit card transactions through the very same processing firm.

5.2. Restricted domain names

One proposed solution to the problem of phishing sites is to create top level domain names exclusive to specific markets. An exclusive .bank domain was proposed by an Internet security researcher in 2007 (Hypponen, 2007) while a similar scheme for political domains was proposed in the Trademark Cyberpiracy Prevention Act, a bill introduced to Congress in 1999, but which failed to pass. That law would have created a second-level domain name under .us, such as .politics.us or .elections.us, exclusively for use by politicians (McCullagh, 2001).

The main problem with the proposal for a restricted domain for political candidates was that administering the domain and verifying applicants is a major task, one which the Federal Election Commission, the logical choice for such a job, was unwilling to take on. "Given the large number of federal, state and local candidates and officeholders, compiling and maintaining a complete list of all persons who are eligible would likely be a sizable undertaking.... The commission does not have the resources to assume responsibility for a task of this magnitude," the FEC said in a March 2000 letter to the Commerce Department. The most the FEC was willing to do, was to compile a list of links to "the official websites of all current federal candidates" and campaign committees (McCullagh 2001).

5.3. Consolidation at the front-end

From a security standpoint, it is far better for candidates to join forces and share one common, trusted brand for their online campaign donations. The current situation in which money, time and other resources are spent creating brand awareness for new campaign websites each election cycle is both inefficient and also makes it extremely difficult for users to develop trust with any one site. Campaign websites simply churn too fast for users to establish trust relationships with them.

One example of brand consolidation is the highly successful Democratic fundraising website ActBlue. The site is popular with left-wing bloggers and netroots organizations and is used to funnel campaign donations for multiple candidates through a single brand. In addition to being used by third party political organizations and activists, it has been adopted by high profile political candidates such as John Edwards, as their official campaign fundraising platform. Users who visit the official Edwards website and click on one of the many "donate" links and buttons will be redirected to a webpage located on the ActBlue website. ActBlue has raised over $29 million since its launch in 2004 (ActBlue, 2007). A similar Republican centralized donation website, RightRoots, was launched in early 2007, although it has yet to achieve ActBlue's level of success.

ActBlue has rapidly become a major source of funding for Democratic candidates. However, it is still unknown to the the general public and to the large numbers of voters who already give money via official campaign websites. To establish a major brand identity, companies typically spend millions of dollars on an advertising campaign. While major political candidates certainly spend millions, their primary

goal is not to establish website brand identity, but to spread recognition and positive feelings for that candidate. It is unlikely that the candidates or anyone else would spend the money required to make ActBlue or RightRoots household names. To do so would simply be an inefficient use of limited campaign funds.

The optimal solution would be for candidates to leverage existing and well known brands that consumers already trust. Online payment systems such as PayPal and Google Checkout are trusted by millions of users with their financial information and transaction history. Similarly, social networking sites such as Facebook and Myspace are trusted with significant amounts of private information, including users' contact lists, personal information and potentially embarrassing photographs.

5.4. Leveraging the existing trusted online payment networks

We propose that PayPal and Google Checkout, the two market leaders in online payment, should create verified political candidate donation sites. Under such a system, the payment companies would permit political campaigns to create fundraising pages hosted within the paypal.com and checkout.google.com branded domains. Before allowing a site to go live, the companies would require the campaigns to submit documentation proving their official candidate status, and would verify that the individuals registering for the sites be authorized to act on behalf of the campaigns. Ideally, the payment websites would establish a consistent URL structure, which would further assist potential donors in verifying that sites are authentic. Examples of such URLs could include:

www.paypal.com/candidates/president/Hillary and
checkout.google.com/politics/senate/Webb, etc.

The major online payment firms already process hundreds of millions of dollars in transactions per year, and do so safely and securely. These companies have spent significant sums in establishing well known, trusted brands, and in getting users to sign up for accounts. By using one or more of these online payment firms, political campaign will be able to leverage the significant economies of scale that PayPal and Google will bring, in terms of existing infrastructure, resources and technical expertise.

Political campaigns that switch to a Google or PayPal hosted solution will find the transaction time for donations will be significantly reduced. This is mainly due to the fact that many customers leave their credit card details on file with the major online payment processors. Thus, for a donor who already has a PayPal account, giving money to a candidate would no longer require that she type in her name, address or credit card information. In addition to reducing the work required to donate, this may result in an increase in donations, as donors will have less time to second-guess their donation during the time that they'd normally be typing in their credit card information. Such a system, while not completely "one click", would definitely result in a more streamlined and user-friendly donation process.

Both PayPal and Google have significant experience in dealing with phishers and other forms of fraud online. PayPal is a frequent target of phishing attacks, while "click fraud" against Google's advertising system is major concern for many in the industry (Liedtke, 2006). As a result, both companies have teams of researchers, engineers and operations staff working in the areas of security and fraud. By using these online payment firms, political campaigns will be able to take advantage of the anti-fraud expertise that the companies possess — a resource they do not currently have access to.

Shifting to the major payment processing companies would provide the campaigns with a number of benefits in terms of security for their donors' financial information. Under the current system of candidates hosting their own donation software, or using niche back-end software suppliers, the possibility exists that donor credit card information can be lost or stolen. Insiders, either in the political campaigns themselves or technical staff managing the web servers can steal data, or insert back-doors into the software code. In the event of an incident of accidental data loss, or data theft by hackers, it is quite likely that consumers would blame the candidates for the loss of their financial data and any associated risk of identity theft. By using a company with a trusted and well known brand to process transactions, the campaign will benefit twofold: First, donors' credit card information will be transmitted directly to PayPal or Google, and as such, there will be no opportunity for campaign insiders to steal the data, nor for hackers to break in later and steal it from the campaign servers. Second, in the event that Google or PayPal get hacked or lose data, the public will most likely blame the payment companies and not the political candidates. It will be Google's brand that suffers, not the politician's.

Finally, the political campaigns should be able to shift to using Google Checkout or PayPal without having to pay any additional costs. Due to the massive number of transactions that the firms process, they are able to offer extremely low transaction fees. As a result, political campaigns would not see an increase in fees, and could actually save money. ActBlue charges campaigns 3.95 percent of the gross contribution amount to cover the credit card processing costs. In contrast, Google Checkout charges merchants 2 percent plus $0.20 per transaction (Google, 2007) while PayPal charges approximately 1.9 percent plus $0.30 cents per transaction, for the transaction levels that most major candidates would achieve (PayPal, 2007).

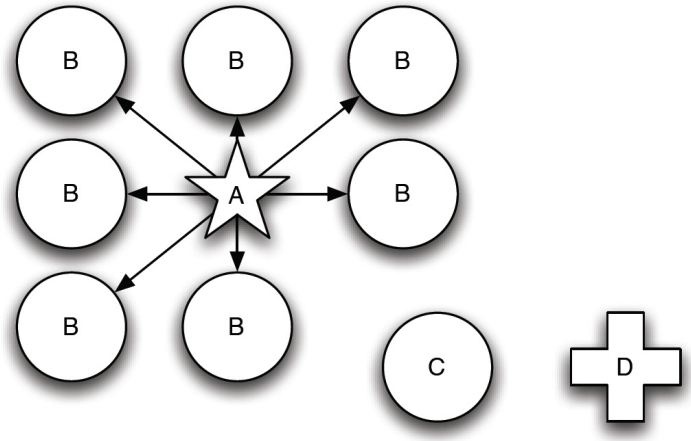

Figure 6: The figure depicts our proposed structure for online donations. Here, a small number of payment aggregators (A) with high brand name and URL recognition allow users to access campaign websites (B) and transfer money to the corresponding campaigns. The malicious payment aggregator (D) has a harder time attracting traffic than in figure 4. This setting therefore is similar to typical phishing attacks against financial institutions.

5.5. Embracing the social networking sites

In addition to entrusting various online payment systems with their financial information, many users also entrust vast amounts of personal information to one or more of the popular social networking websites. Facebook and MySpace, two of the most popular social networking websites, have in 2007 become key platforms to reach younger voters.

In an attempt to communicate the importance of their website to politicians, executives from Facebook held a one day workshop for nearly 200 political campaign staffers in October of 2007. The sessions concentrated mostly on ways which political campaigns could use the social networking site to reach younger voters. Facebook executives noted that of the site's 45 million active users, 80 percent are of voting age (Friere, 2007). Users of the social networking site can add a candidate as a "friend" and stay virtually connected to that candidate's campaign. They can also add more than 190 political applications – like a 2008 voter registration form – to their profiles (Vargas, 2007a). Some Facebook groups rallying users for and against individual candidates have over 500,000 subscribed users. A group created to support the short-lived presidential candidacy of TV comedian Stephen Colbert was able to attract over 1.2 million Facebook users in less than 12 days (Vargas, 2007a).

Rupert Murdoch's MySpace also is doing its best to become part of the political process. The website has partnered with the MTV television station to host "instant

message forums," a televised town meeting of sorts with a studio full of young people, but also permitting MySpace users to submit questions to the candidates over the company's website (Vargas 2007b). In October 2007, the website also announced a partnership with PayPal to allow candidates to accept campaign donations directly from their respective MySpace profile pages. The transactions, of course, are processed by PayPal. Some major candidates, including Rudy Giullani, use the system. This donation system is promoted as a means of reaching younger audiences, and any potential anti-phishing benefits are not mentioned in materials describing the program (MySpace 2007).

The major social networking sites, as they currently function, are not yet the perfect solution for candidates' campaign donation needs. All users, be they college students or presidential candidates, are limited to the amount and kinds of content that they can display on their pages. Facebook users do not have memorable profile URLs. For example, Barack Obama's Facebook profile is located at www.facebook.com/person.php?id=2355496748 - which is not something that could be printed on a campaign sign or a bumper sticker. MySpace is closer to being useful enough for candidates to print on a poster. Candidates get memorable URLs, for example www.myspace.com/barackobama, and the candidates can embed far more of their own content, images and video onto the page than the strict limits that Facebook sets for its profiles. However, in spite of these benefits, the candidates' MySpace profiles still look like so many other MySpace profiles on the social networking site: garish, cluttered, and confusing. It is not possible to use the candidate's social networking profile to learn about their positions on important issues, or to learn much about them beyond the basics. For that depth of information, potential voters need to visit the official campaign websites.

6. Conclusion

This paper has discussed the vast sums of money that are currently flowing to candidates via online donations. Political campaigns encourage extremely risky behavior on the part of the user in order to get the best response from their mass-email solicitations. Users are being trained to click and donate when they receive political emails, while at the same time banks and other financial firms are doing everything possible to stop users from clicking on links in email messages. Furthermore, the fact that there are so many different candidates, and no consistent domain name scheme for politicians means that most users simply cannot be expected to know when they are at a valid political website or not.

These and other factors combine to make the threat of political phishing a serious one. The safe way forward is for politicians to partner with existing trusted brands such as Google, PayPal, Facebook or MySpace. These firms are already household names and are trusted by many users enough that the users allow the sites to store their credit card details as part of their account information. The payment companies in particular have significant expertise in security and fraud — something that none of the candidates currently have.

Left ignored by the candidates and campaigns, the theoretical threat of political phishing will almost certainly become a reality. There is just too much money to be made by criminals for them to overlook the opportunities made possible by political deception forever.

References

ActBlue (2007), "The online clearinghouse for Democratic action," www.actblue.com, (Accessed 10 December 2007).

Edsall, T. B. (2006), "Rise in Online Fundraising Changed Face of Campaign Donors," *The Washington Post*, www.washingtonpost.com/wp-dyn/content/article/2006/03/05/AR2006030500816.html, (Accessed 10 December 2007).

Experian (2007), "National Score Index," www.nationalscoreindex.com/, (Accessed 10 December 2007).

Felten, E. W. and Schneider, M. A. (2000), "Timing attacks on web privacy," *CCS '00: Proceedings of the 7th ACM conference on Computer and communications security*, New York, NY, USA, pp. 25–32, ACM Press.

Friere, J. P. (2007), "Facebook Pitches Its Political Benefits," *The New York Times — The Caucus*, thecaucus.blogs.nytimes.com/2007/10/10/facebook-trains-campaigns-to-use-the-web/, (Accessed 10 December 2007).

Goodin, D. (2007), "Yahoo feeds Trojan-laced ads to MySpace and PhotoBucket users," *The Register*, www.theregister.co.uk/2007/09/11/yahoo_serves_12million_malware_ads, (Accessed 10 December 2007).

Google (2007), Google Checkout Fees, checkout.google.com/seller/fees.html, (Accessed 10 December 2007).

Hermida, A. (2004), "E-mail scam plays on US elections," *BBC News Online*, news.bbc.co.uk/2/hi/technology/3714944.stm, (Accessed 10 December 2007).

Hypponen, M. (2007), "21 solutions to save the world: Masters of their domain," *Foreign Policy*, www.foreignpolicy.com/story/cms.php?story_id=3798, (Accessed 10 December 2007).

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007), "Social phishing," *Commun. ACM*, **50**, 94–100.

Jakobsson, M. (2007), "The Human Factor in Phishing," *Privacy & Security of Consumer Information*, www.informatics.indiana. edu/markus/papers/aci.pdf, (Accessed 10 December 2007).

Jakobsson, M. and Stamm, S. (2006), "Invasive browser sniffing and countermeasures," *WWW '06: Proceedings of the 15th international conference on World Wide Web*, New York, NY, USA, pp. 523–532, ACM Press.

Krebs, B. (2006), "Hacked Ad Seen on MySpace Served Spyware to a Million," *The Washington Post — Security Fix*, blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html, (Accessed 10 December 2007).

Krebs, B. (2007), "Virus Writers Taint Google Ad Links," *The Washington Post — Security Fix*, http://blog.washingtonpost.com/securityfix/2007/04/virus_writers_taint_google_ad.html, (Accessed 10 December 2007).

Liedtke, M. (2006), "Click fraud concerns hound Google despite class-action settlement," *The Associated Press*, www.post-gazette.com/pg/06135/689369-96.stm, (Accessed 10 December 2007).

McCullagh, D. (2001), "Satirists Didn't Steal Election," *Wired News*, www.wired.com/politics/law/news/2001/01/41293, (Accessed 10 December 2007).

McCullagh, D. (2003), "Bush OKs spam bill–but critics not convinced," *CNET News.com*, www.news.com/2100-1028-5124724.html, (Accessed 10 December 2007).

Murota Laboratory — Tokyo Institute of Technology (2006), "Scrapbook Firefox Extension," amb.vis.ne.jp/mozilla/scrapbook/, (Accessed 10 December 2007).

MySpace (2007), "MySpace Teams with PayPal, Empowering Non-Profits and Political Candidates to Virally Fundraise," *Press Release*, biz.yahoo.com/bw/071004/20071004005964.html?v=1, (Accessed 10 December 2007).

National Geographical and Political Software (2007), "Our clients," www.ngpsoftware.com/clients, (Accessed 10 December 2007).

PayPal (2007), "Transaction Fees --- PayPal," www.paypal.com/cgi-bin/webscr?cmd=_display-receiving-fees-outside, (Accessed 10 December 2007).

Raney, R. F. (1999), "Bush campaign asks government to go after critical web site," *The New York Times*, www.nytimes.com/library/tech/99/05/cyber/articles/21bush.html, (Accessed 10 December 2007).

Seltzer, L. (2004), "Spotting Phish and Phighting Back," *eWeek.com*, www.eweek.com/article2/0,1759,1630161,00.asp, (Accessed 10 December 2007).

Soghoian, C. (2007), A Deceit-Augmented Man In The Middle Attack Against Bank of America's SiteKey Service. *Slight Paranoia*, paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html, (Accessed 10 December 2007).

Srikwan, S. and Jakobsson, M. (2007), "A consumer security awareness campaign based on cartoons," www.securitycartoon.com, (Accessed 10 December 2007).

Stirland, S. L. (2007), "Scoop: Clinton raised $8 million online in 3Q," *Wired News — Threat Level*, blog.wired.com/27bstroke6/2007/10/scoop-clinton-r.html, (Accessed 10 December 2007).

Swartz, J. (1998), "Government parasites — 'stealth' web pages feed off addresses," *San Francisco Chronicle*, www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1998/06/03/BU29204.DTL, (Accessed 10 December 2007).

Vargas, J. A. (2007a), "The Colbert Clan: 1.2 Million Strong and Counting," *The Washington Post — The Trail*, blog.washingtonpost.com/the-trail/2007/10/30/the_colbert_clan_12_million_st.html, (Accessed 10 December 2007).

Vargas, J. A. (2007b), "MTV Turns Out to Be Obama's Space," *The Washington Post — The Trail*, blog.washingtonpost.com/the-trail/2007/10/29/post_160.html, (Accessed 10 December 2007).

Wolf, Z. B. and Parker, J. (2007), "Paul Calls $4M Haul 'Remarkable,'" *ABC News*, abcnews.go.com/Politics/Vote2008/Story?id=3826332, (Accessed 10 December 2007).