About-Us/Project-History.aspx (Accessed November 2012).
Pew Research Center. "About: Andrew Kohut." http://www.people-press.org/about/andrew-kohut (Accessed November 2012).
Pew Research Center. "Pew Charitable Trusts Establishes New Nonprofit Research Organization to Help Better Inform Public and Policy Makers on Key Issues and Trends." http://pewresearch.org/docs/?DocID=142 (Accessed November 2012).

Phishing, Political

Phishing is the act of enticing a person into revealing private information by masquerading as a trustworthy entity. Phishing can be used to steal any type of restricted information (e.g., money, hospital records), and can be accomplished through any communication technology (e.g., e-mail or voicemail), as well as in person. In the political realm, phishing refers to the theft of personal information by masquerading as a political entity, most commonly a politician running for office who requests donations from supporters. In this case, the victim gives money to the phisher, rather than to the politician. As a result, both the campaign donor and the legitimate politician who might have benefited from the donation are defrauded.

Political phishing can also refer to conning politicians and government officials into disclosing confidential information, such as national security intelligence and plans for political campaigns, which can then be used for terrorism, espionage, or sabotage. Studies show that phishing is prevalent in the United States and results in substantial monetary damages, although there are no such statistics currently available on political phishing in particular.

Several remedies have been proposed to reduce the impact of phishing attacks. These include both technical solutions (i.e., developing blacklists of phishing sites and removing them from the Internet, building better antispyware software) and user education programs on how to recognize fraudulent e-mails and Web sites. Both have shown effectiveness.

The term *phishing* is believed to be a word play on "fishing," because it refers to the baiting of individuals through illicit messages, with the initial letters standing in for "password-harvesting." The majority of phishing attacks are perpetrated over e-mail, with phishers pretending to be a bank or financial institution, and requesting users to login to their accounts in order to verify information or change their personal identification numbers (PINs).

The e-mail directs users to a fraudulent Web site, where their private information is captured and later used to steal money. Another common phishing technique is installing malicious software (malware) on users' computers when they simply click on a fraudulent Web site or open an infected e-mail attachment. The malware then steals private information from users' computers through key logging or downloading Internet browsing caches. The most successful type of phishing, known as "spear-phishing" because of its highly targeted nature, involves including some personal information, such as names, dates of birth, and the last four digits of credit card numbers, in e-mails sent to potential victims. The users interpret this information as a sign of e-mail credibility, when in fact it is mined from the Internet by the phishers, or is simply made up.

Political Phishing

Campaign donations are a particularly ripe target for e-mail phishing. First, politicians have exempted their campaign donation solicitation e-mails from the CAN-SPAM Act, which prohibits the promotion of commercial products and services through unsolicited e-mail. As a result, the public is less suspicious of receiving campaign donation requests from politicians via e-mail. Second, political domain names tend to fluctuate, which makes the public less able to distinguish between real and fake ones. For instance, President Barack Obama may use barack4president.com, obama12.com, or barackobama.com. All of these Web sites appear legitimate, yet some of them may be phishing scams. By contrast, financial institutions maintain strict consistency in their domain names precisely in order to avoid confusion between their real Web sites and a phishing impersonator. Third, it is relatively easy to mine for information about political affiliation in

order to create personalized spear-phishing campaigns. This information can be found on social network sites or on records of individuals' prior campaign contributions, which are publicly available online, as required by law. Finally, political phishing may be less detectable than other types of phishing. Provided that phishers do not steal more money than the intended campaign contribution, the victims may not even realize that they have been defrauded. Political phishing Web sites may then be less likely to be blacklisted and taken off the Internet.

To combat political phishing, politicians have adopted two noteworthy tactics. One is brand consolidation, or funneling campaign donations for multiple politicians through a centralized donation Web site, the Democratic ActBlue and the Republican RightRoots. The other is enabling donations through users' existing accounts with PayPal and Google. These strategies help avoid confusion between candidates' domain names, and forgo the necessity of inputting financial information for every donation, thus reducing contributors' susceptibility to phishing scams.

Catalina L. Toma
University of Wisconsin–Madison

See Also: Campaigns, E-Mail; CAN-SPAM Act; Data Mining; Decoy Campaign Web Sites.

Further Readings

McGrath, Kevin and Minaxi Gupta. "Behind Phishing: An Examination of Phisher Modi Operandi." In *Proceedings of the 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats*. Berkeley, CA: USENIX Association, 2008.

Ratkiewicz, Jacob, et al. "Detecting and Tracking Political Abuse in Social Media." Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, 2011. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274 (Accessed November 2012).

Soghoian, Christopher and Markus Jakobsson. "The Threat of Political Phishing." In *The Second International Symposium on Human Aspects of Information Security & Assurance,* Nathan Clarke and Steven Furnell, eds. Plymouth, MA: University of Plymouth, 2008.

Picasa

The proliferation of broadband Internet, digital cameras, and smartphones has made photo sharing a popular communication practice. Picasa is Google's Web- and desktop-based application for sharing digital photographs. Created by Lifescape, initially Picasa was a software package for organizing and storing photos for Microsoft Windows. In 2004, Google acquired Picasa from Lifescape, released it free of charge, and developed it for Windows, Mac operating system (iOS), and Linux. Picasa is a part of Google's attempt to establish an entire ecosystem of software services that include social networking, e-mailing, photo sharing, and file or document sharing. The role of Picasa in this all-inclusive system is to act as a hub for the storage and circulation of photos. Any Google service that can carry image-based content will automatically sync with the user's Picasa account. For example, files stored on Picasa can be uploaded to another Google service, such as Blogger, while any files uploaded to Blogger will automatically appear on the user's Picasa account, and can then be recirculated to another service such as the social network Orkut.

In addition to making the software available across a range of operating systems, Google developed Picasa Web, the online portal of Picasa. Most users use Picasa Web to upload, store, and share their photos in photo albums. Like many other forms of social media, Picasa's organizational structure works with tags, which are searchable by the general public. Users can disseminate the content of their photos in several ways. For example, customized user-generated tags let Picasa users browse through their photo albums or other people's photo collections in an associational way. Users can also contribute to threaded discussions regarding photo content by making comments and sharing photos on their other Google accounts, thereby generating traffic. This networking functionality allows users to partake in a form of asynchronous social interaction around photos in the online domain. Similar to Flickr, the threaded discussion acts as an archive of social interaction that can be added to at various times.

Image-centric social media developments such as Picasa are changing both online and offline