Can spyware be disguised within emails, social media, web chats etc?

McCann Investigations
1018 Preston St.
Houston
TX 77002

Table of Content

Can spyware be disguised within emails, social media, web chats etc? Short Answer, Yes.. Read More

Emails, social media, web chats and other methods of communicating online are now one of the most used aspect of internet for users. To put this into perspective in 2015[1], out of the total world population of 7.2 billion, 3.01 billion use the internet and 2.01 billion of them have active **social media accounts i.e. approximately 30%** and 3.65 billion i.e. **51% are mobile users**. This makes 30-51% connected users vulnerable to spyware and phishing online.

These attacks can be either personal or mass targeted. There are different kind of spyware, from ones that run in the background, gathering user information to simple ones, which ask for the information from users.The most used and well-known method of **targeted spyware is phishing**. Phishing[2] is a technique that uses spam, malicious websites, email messages and instant messages, social media and other tools to trick people into divulging sensitive information with immediate profit potential.

A common phishing method is to collect sensitive information by *pretending* to be a trustworthy entity. For instance, posing as a legitimate source, requesting personal information through email[3] and directing recipients to fake sites to enter their data gives phishers access to the exact kind of information they are looking for, most commonly financial information. This information is then used to impersonate the victim and actually steal their money.

However, the world of phishing is very broad, from attacks targeting **tens of thousand of potential victims** at once, to focusing on a single individual at a time. Google recently published a study[4] demonstrating that **manual phishing attacks**, the ones that don't use any automated tools, and simply spend time profiling their targets, are the simplest and most effective method for hacking email accounts.

A good **example[5]** of manual targeted phishing is this: the attacker scans a social network site, finds a potential target, finds a list of friends and a reference to a cool device the target has just bought at an online retail site. Using this information, a spear phisher could pose as a **service assistant from the vendor**, asking the target to confirm credit card data or change the password, allowing him access to the victim's financial information.

---

[1] Source: http://www.slideshare.net/fullscreen/wearesocialsg/digital-social-mobile-in-2015/6

[2] Source: http://www.phishing.org/phishing-techniques/

[3] Source: http://www.phishing.org/scams/email-phishing/

[4] Source: http://securityaffairs.co/wordpress/30020/cyber-crime/manual-phishing-attacks.html

[5] Source: http://us.norton.com/spear-phishing-scam-not-sport/article

Phishing can also be very effective when using more interactive means, like **instant messaging or web chat** and tricking the user into believing that the attacker is a service provider, usually a live chat[6] disguised as support service for a big e-commerce company or software company. By asking the right questions, an attacker can acquire the victim's credentials and access the financial information linked with the victim's actual account.

Basically any form by which the perpetrator can legitimate its action of asking for **personal information** can be used, from email to web chat and messaging, to social media interaction or using the contacts of a victim to pass on the fraud. Attackers usually take advantage of the **cyber context** to substantiate their request for information. For instance, a lot of last year's phishing attempts used the general panic regarding the **Heartbleed vulnerability[7]** in the popular **OpenSSL cryptographic software[8]** library to ask victims to change their passwords or other account information in order to protect their potentially exposed personal and financial information.

[6] Source: http://news.netcraft.com/archives/2013/05/07/live-chat-used-in-phishing-attack.html

[7] Source: http://tech.firstpost.com/news-analysis/new-phishing-scam-exploits-heartbleed-fear-to-con-users-222657.html

[8] Source: http://www.computerworld.com/article/2490169/security0/phishing-campaign-touts-fake--heartbleed-removal--tool.html


MCCANN INVESTIGATIONS
EST. 1984
TOTAL SECURITY SOLUTIONS