Following global trends in online threats, the RSA Anti-Fraud Command Center continues to see large increases in phishing attacks. Looking back to the first half of 2012 and comparing it with the second half of 2011, RSA reported a 19% increase in global phishing attacks. Not only is phishing still rampant, it is resulting in significant losses to global organizations. RSA estimates that phishing cost organizations an estimated $2.1 billion in losses over the last 18 months. Instead of going away, phishing is stronger in numbers and resulting in more losses. And although this threat is more familiar than ever to online users, it still appears to work.

Phishing is, in a sense, nothing more than the old confidence scam, only nowadays the deception happens online. Preying on human emotion is as primal a tactic as it gets and mainly what keeps phishing alive. Beyond luring victims with greed (awards and winnings-themed phishing emails) or anxiety (your-account-will-be-blocked-titled phishing scams), phishing preys on trust in more ways than one. And where better would one find trust than among people who know one another – on a social networking site.

PHISHING AND THE SOCIAL WORLD

Just four years ago, slightly more than 20% of U.S. citizens were users of social networks. That number has since more than doubled and stands at around 50% today. Facebook membership alone has increased nearly 10 times since 2008 and Twitter shows that membership has increased by a factor of five over the same period.

With the world turning into a smaller and more 'social' village, fraudsters and blackhats are certain to join the party. Cybercrime follows the money, and as user behavior shifts, fraudsters have been following their target audience (potential victims) to the virtual world’s hot spots. According to a research study by Microsoft, phishing via social networks in early 2010 was only used in 8.3% of all attacks—by the end of 2011 that number stood at 84.5% of attacks delivered through social media.
WHAT'S SO GREAT ABOUT PHISHING VIA SOCIAL MEDIA?

Using social networks, people behave more socially and are less discriminating with messages or comments they receive on their profiles. With new user numbers soaring every year, phishers get to cast a very wide net. One phishing attack tailored for the look and feel of a single social network can effectively target a very large amount of people, resulting in less work for the fraudster to do and a better yield of potential victims.

With social media, a core component of a successful phishing attack is already built-in: Trust. Users ‘follow’ people they know or trust, they receive messages from people or services they are familiar with (emails from a site’s team for example, a group, a friend’s hijacked account, or comments containing poisoned links).

Rogue communications can sometimes be visually spotted, but most times they look good enough to have the recipient click and go to the phishing site or download a malicious piece of software. In cases where a social network makes heavy use of URL shorteners, telling a suspicious hyperlink before browsing to it is very difficult.

IT ONLY GETS BETTER (FOR PHISHERS)

Social networking sites are getting much better at knowing their users and leveraging that information for more targeted marketing and sales. One of the factors that help enhance the credibility factor in the ever-evolving social media platform is the emerging Freemium model.

Perhaps one of the most popular activities on some social networks is playing social games with other users. The games are free, but only until the user wants to really get ahead in the game or obtain special powers upgrades. This is where the payment prompt jumps in, suddenly making it okay to perform financial transactions through a platform like Facebook.

What does this mean for the user? It legitimizes using their credit card details on the social networking site.

What does this mean for phishers? More ways to phish, more data to steal (alongside all the other personal information already shared by users), more attacks and more successful phishing!

Another factor that has been encouraging phishing to come through social networks is enterprises going social. For example, banks that wish to market themselves using social media open user groups people can join, inadvertently providing phishers with a model to follow (not any different from online banking portals being imitated for phishing).

As with any online-borne threat, keeping a close watch on trends is essential to any organization serving customers via the Internet. This new and increasingly ‘social’ nature of delivering phishing attacks is a reflection of user behavior – a factor that will always be the most significant driver for online crime trends.

Growing use of social networking is going to make phishing via that media more popular with time, and just further supporting the need for ongoing and timely user-education and awareness campaigns to help consumers protect their online identities and accounts.
Phishing Attacks per Month
In September, RSA identified 35,440 phishing attacks launched worldwide, marking a 28% decrease from August. RSA data shows that the bulk of this decrease is a result of fewer phishing campaigns launched against a series of European financial institutions, which have accounted for significant spikes in attacks through the past few months.

Number of Brands Attacked
In September, 314 brands were targeted by phishing attacks, marking an 8% increase from August. Increases in the number of brands attacked suggests cybercriminals are casting wider nets at organizations that may not be as well protected or are less familiar with the threat.
Top Countries by Attack Volume

Despite a 22% decline in attacks, the UK continues to be the country that endured the highest attack volume – marking the seventh consecutive month – with 47% of attack volume. In turn, Canada absorbed most of this with 17% of attack volume in September.

US Bank Types Attacked

In the U.S. banking sector, nationwide bank brands witnessed a 10% increase in attacks – accounting for about three out of every four attacks in September. This is not surprising as phishers tend to seek a brand that is well-known and has multiple locations within a region, such as nationwide banks. In this case, there is a larger pool of potential victims and the chance of a spam recipient being an account holder of the targeted brand is much higher.
Top Countries by Attacked Brands

In September, U.S. brands continued to be the most targeted by phishing – targeted by 29% of attack volume, followed by the UK and Australia.

Top Hosting Countries

In September, the U.S. continued to be the top hosting country for phishing attacks hosting 77% of attacks. Poland, the UK, Canada, and France accounted for hosting just over 10% of attacks in September.
CONTACT US
To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa

©2012 EMC Corporation. EMC, RSA, the RSA logo, and FraudAction are trademarks or registered trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned are the property of their respective holders. OCT RPT 1012