WHITE PAPER

Cyveillance®

The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks

A Cyveillance Report
October 2008

EXECUTIVE SUMMARY

How much do phishing attacks really cost organizations? This question has intrigued and frustrated the security industry since attacks began to appear. According to Gartner study released in December 2007, phishing attacks represent a staggering amount of fraud, costing organizations more than 3 billion dollars annually. Even more shocking than this cost is the fact that phishing is a steadily growing problem with no end in sight.

This increase in phishing is hardly a surprise, as this form of online fraud has grown into one of the most common and most profitable scams for criminals. The schemes vary, but they typically involve using some combination of spoofed junk email (spam), malicious software (malware), and fake Web pages to harvest personal information from unwitting consumers. Customers of both well-known brands and lesser-known companies alike have fallen victim to this pervasive form of online fraud. In fact, over the past three years, Cyveillance, the world leader in cyber intelligence, has detected phishing attacks against more than 2,000 brands across 30 countries.

Organizations often have a difficult time assessing how phishing affects their finances, as there are numerous factors to take into account when trying to measure the cost as well as the impact phishing has on customers, productivity and reputation. In this document, Cyveillance's phishing experts explain the costs of phishing attacks, in a manner that can be easily adjusted to any organization's specific business model or support process.

THE COSTS

Phishing attacks can cost organizations anywhere from thousands to millions of dollars per attack in fraud-related losses. Although some of the costs can be measured easily, others are far more difficult to quantify. The two categories of costs that phishing affects are usually referred to as hard costs and soft costs.

Hard costs associated with phishing can be measured directly in terms of dollars, time and effort. Typically, these costs are related to the following:

- Fraudulent charges associated with the compromised credit card
- Cash withdrawals or "pump and dump" from compromised accounts
- Employee time spent dealing with the fraudulent transactions
- Customer support calls

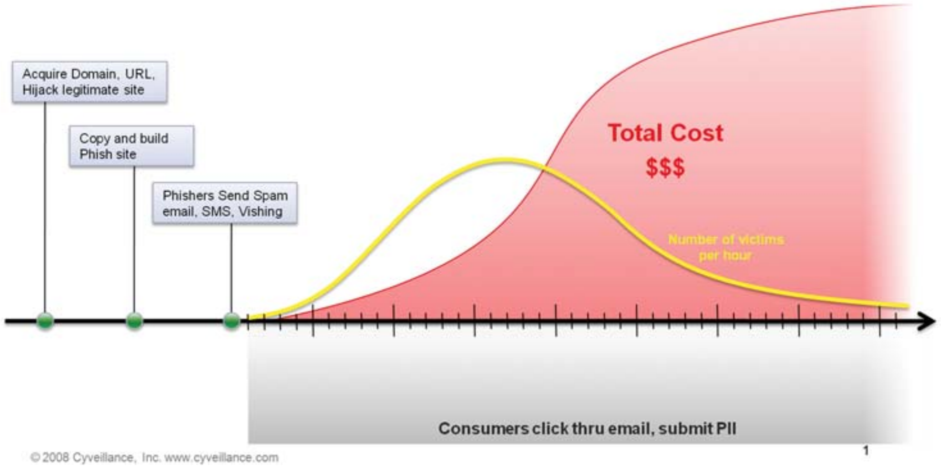
Soft costs are the intangible costs that are much more difficult to measure. These costs can have a long-term impact on an organization's brand. Soft costs typically include the following:

- Customer trust in online applications
- Customer satisfaction
- Reputation

HOW TO ESTIMATE THE COST OF AN ATTACK

There are many factors to consider when estimating the costs of a phishing attack. To provide an approach that produces a realistic estimation, below is an example of a typical attack.

The graphic below illustrates the basic anatomy of a phishing attack. As it clearly shows, the costs dramatically increase as the attack continues and the greatest cost savings occur if the attack is stopped quickly. The following example will show explicit details of how the costs easily escalate.



© 2008 Cyveillance, Inc. www.cyveillance.com

Figure 1

Malware-based phishing is any type of phishing attack that attempts to download malware to a user's machine. Traditional phishing attacks typically only provide a phisher with a single compromised credential or set of compromised credentials that are only valid for a short period of time. Malware-based attacks download malicious software to a user's computer that may go unnoticed for an extended period of time. This software steals sensitive information or allows a fraudster to gain unauthorized access to not only the user's computer, but to any network resource the user can access.

In our example 2,500 users were victim to the phishing attack. If the same phishing attack was malware-based, then up to 25,000 users could be infected with malware. The reason for such a larger exposure is that with a malware-based attack, the user simply has to click on the link to the phishing Web site; he or she will be exposed to the malware infection regardless of whether or not credentials are given to the scam.

In our example (Figure 2) we start with the number of emails spammed by the phisher, which is usually very high. From this initial mailing, we estimate that 10% or fewer of the emails actually pass through anti-spam systems. Of the 10% that pass through these filters, half will be opened by users. As shown in the example below, 10% of the individuals who open the emails will click on the link(s) contained in an email, and of those who click on the link(s), only 10% will actually fall for the scam by entering their personal credentials into the fraudulent Web page. Although this may seem like a small percentage, the actual number of people affected is substantial, as the number of spam messages that the phisher sends during the initial attack tends to be quite large.

Figure 2

Emails Spammed	5,000,000
Percent filtered by spam filters	90%
Percent of people who GET the email that will EVENTUALLY open the email	50%
Percentage of those who will read the email and click on the link to the attack Web page	10%
Of those who clicked on the link, % that fall for the attack	10%
Total Number of people successfully phished	2,500

Cost Assumptions*:

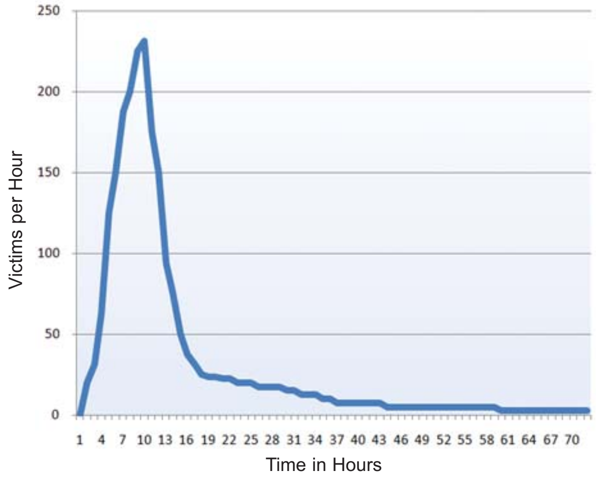
Cash cost per customer compromised	$1,800.00
Personnel per-hour costs for each hour a site is up	$400.00

*The cost assumptions above are based on input and feedback from financial institutions of varying size. Many organizations have their own specific values for the average costs of credentials (login, credit card, etc...) compromised by a criminal and the per-hour costs of responding to an attack.

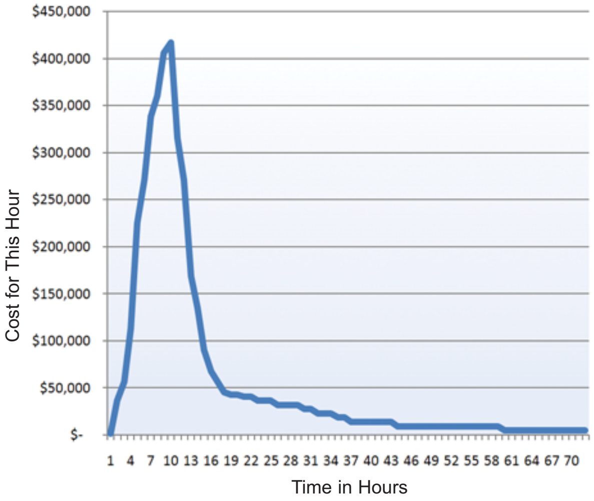
Attack Details:

Hour	% of all victims scammed who are scammed during this hour of the attack	Victims during this hour	Cumulative victims to date	Cost for this hour	Cumulative Cost over the first 72 hours
1	0.03%	0.625	1	$ 1,525	$ 1,525
2	0.80%	20	21	$ 36,400	$ 37,925
3	1.25%	31.25	52	$ 56,650	$ 94,575
4	2.50%	62.5	114	$ 112,900	$ 207,475
5	5.00%	125	239	$ 225,400	$ 432,875
6	6.00%	150	389	$ 270,400	$ 703,275
7	7.50%	187.5	577	$ 337,900	$ 1,041,175
8	8.00%	200	777	$ 360,400	$ 1,401,575
9	9.00%	225	1,002	$ 405,400	$ 1,806,975
10	9.25%	231.25	1,233	$ 416,650	$ 2,223,625
11	7.00%	175	1,408	$ 315,400	$ 2,539,025
12	6.00%	150	1,558	$ 270,400	$ 2,809,425
13	3.75%	93.75	1,652	$ 169,150	$ 2,978,575
14	3.00%	75	1,727	$ 135,400	$ 3,113,975
15	2.00%	50	1,777	$ 90,400	$ 3,204,375
16	1.50%	37.5	1,814	$ 67,900	$ 3,272,275
17	1.25%	31.25	1,846	$ 56,650	$ 3,328,925
18	1.00%	25	1,871	$ 45,400	$ 3,374,325
19	0.95%	23.75	1,894	$ 43,150	$ 3,417,475
20	0.95%	23.75	1,918	$ 43,150	$ 3,460,625
21	0.90%	22.5	1,941	$ 40,900	$ 3,501,525
22	0.90%	22.5	1,963	$ 40,900	$ 3,542,425
23	0.80%	20	1,983	$ 36,400	$ 3,578,825
24	0.80%	20	2,003	$ 36,400	$ 3,615,225
----	-----	----	-------	------------	-----------------
----	-----	----	-------	------------	-----------------
----	-----	----	-------	------------	-----------------
----	-----	----	-------	------------	-----------------
----	-----	----	-------	------------	-----------------
48	0.20%	5	2,258	$ 9,400	$ 4,083,825
----	---	----	------	-----------	-----------
----	---	----	------	-----------	-----------
----	---	----	------	-----------	-----------
----	---	----	------	-----------	-----------
----	---	----	------	-----------	-----------
72	0.10%	2.5	2,346	$ 4,900	$ 4,250,925
	93.8%	2346	4,691	$ 4,250,925	$ 4,250,925

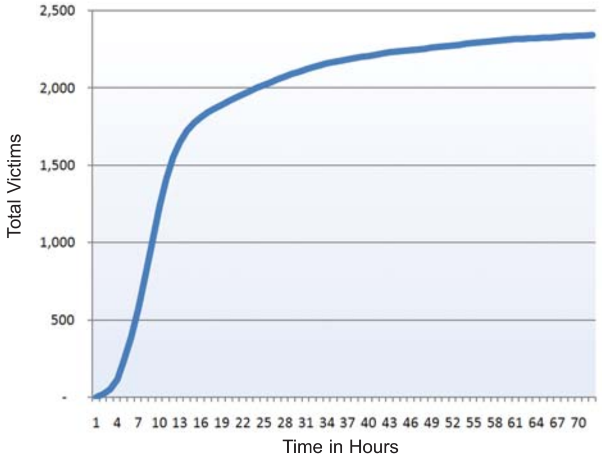
Victims per Hour for the First 72 Hours



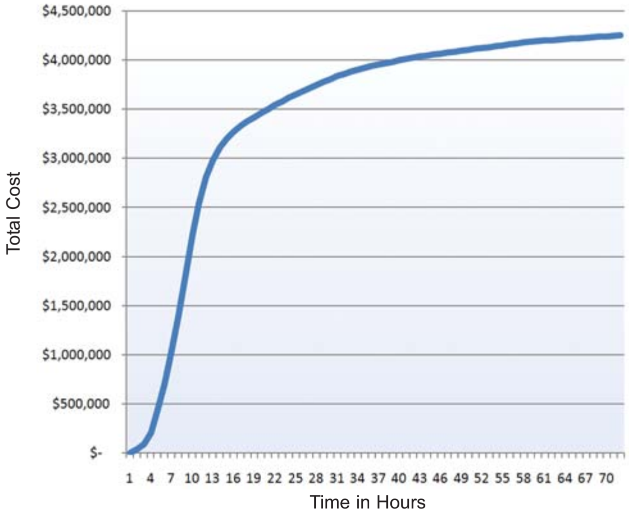
Totel Cost per Hour for the First 72 Hours



Cumulative Victims Over the First 72 Hours



Cumulative Cost Over the First 72 Hours



The duration of the phishing attack is a key factor in determining the overall costs of a specific attack. As specifically illustrated in the attack detailed above, we can ascertain that the majority of costs associated with a phishing attack occur within 24 hours of the attack's launch and that after that period, the costs associated with an attack level off significantly.

REDUCING THE COSTS OF ATTACKS

Any organization currently targeted by phishers or at risk for such attacks must develop and implement a comprehensive phishing protection and response plan in order to prevent or minimize the direct costs of phishing attacks. The plan should provide response guidelines that cover every phase of an attack in the fastest, most efficient manner.

Based on the analysis in the previous section, we note that most costs are incurred during the first 24 hours of an attack. Because of the length of this critical period, speed of detection and takedown of the attack are the two key areas that organizations must focus on to reduce the costs of a phishing attack. Organizations should place equal emphasis on both areas when developing and implementing a phishing protection and response plan.

An effective phishing protection and response plan should include the following key objectives:

- Identification of the appropriate stakeholders and clear communication of their responsibilities
- Compatibility with existing processes and procedures (Your plan must work within the daily operational flow of business.)
- Creation of effective internal and external communications processes
- Creation of a solid phishing response escalation path
- Minimization or avoidance of negative customer experiences (Preserving consumer confidence in using online services is crucial to ensure continued growth.)
- Reduction of financial losses associated with online fraud
- Proactive protection of your corporate reputation

Depending on the size of an organization and the availability of resources, the best decision may be to outsource the core parts of phishing detection and response. An anti-phishing service provider should easily be able to reduce the costs of phishing significantly.

CONCLUSION

Phishing is a problem that will grow and evolve over the foreseeable future, as criminals will continue to use the scams as an effective means of generating significant profit. The attacks constantly adapt to technology, becoming more sophisticated in an attempt to outpace countermeasures for detection. Phishing attacks not only have increased substantially the costs associated with running a business, but also have affected security and customer confidence negatively.

While there is no silver bullet to eliminate all costs associated with phishing, organizations can focus on addressing attacks during the most dangerous time, the 24 hours following the launch of the attack. The costs associated with a phishing attack are directly proportional to the amount of time that it takes an organization to approach the attack. Thus, the better prepared an organization is to detect and take down phishing attacks proactively, the more likely that the organization will be able to prevent and/or recover from attacks. By trying to nip the problem in the bud, an organization can greatly reduce the amount of time wasted and money lost due to a potential phishing attack.

ABOUT CYVEILLANCE

Cyveillance offers the industry leading Anti-phishing solution that will proactively address this growing threat with an intelligence-led approach to security – one that can identify risks early for effective prevention and resolution. Cyveillance Anti-Phishing can help you quickly identify, shut down and recover from online scams that mislead customers through fraudulent use of their corporate identity.

Cyveillance is the only company to offer a guarantee for phishing site take-downs – we take it down in five hours or less or you don't pay for it -- to ensure minimal losses for your organization and customers. To learn more about how you can cut losses from phishing attacks visit www.cyveillance.com or call today, toll free, 1.888.243.0097.

Cyveillance, Inc,
1555 Wilson Boulevard
Suite 406
Arlington, VA 22209-2405
888.243.0097
www.cyveillance.com
info@cyveillance.com