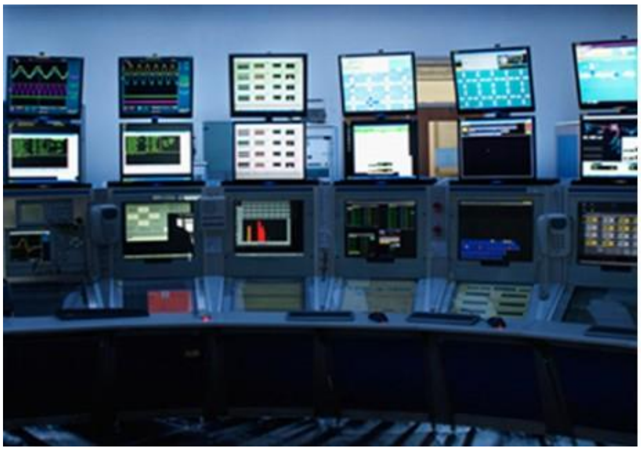
Deloitte.

Risk Services
January 2015



Abuse of your company's corporate identity with phishing emails

How to defend your corporate reputation

Organizations are often directly targeted by phishing emails by attackers. These attacks usually aim to trick an employee to disclose access credentials or to share sensitive information. Besides resolving this challenge, organizations are now facing a second challenge: attackers start abusing their brand name to gain trust at the companies' most important segment: the customer. According to a report of the Anti-Phishing Working Group (APWG)[1], on average 312 brands are abused every month by phishers (Q2 2014).

Brand names and logos are often used in the email itself, but also at counterfeit phishing websites, with the goal to win the trust of the customer and steal information or spread malicious software. **The financial industry is most targeted, with 40% of all attacks in Q2 2014.** Attackers use the bank logos since customers are most susceptive when their financials are jeopardised. If someone receives an alarming email about a payment being blocked by their bank due to a security issue, customers are triggered to click the link or open that attachment. As the financial sector is targeted most, customers may not think of phishing the moment they receive an email from a company outside the financial sector. Therefore, companies located outside of this sector which do handle important data should be keen on proactively spotting phishing and informing their consumers.

If you are a big organization chances are also higher that consumers will receive emails supposedly send by you, with your brand name and logo on it. Whether or not your customers fall for the bait, they will consequently be more suspicious of emails send by you and might develop a negative association with your brand. How can you make sure your customers recognize these phishing emails and protect your reputation at the same time?

[1] Anti-Phishing Working Group (2014). Phishing Activity Trends Report 2 Quarter, (June).

1.Prevent phishers using your brand
2.Make sure your customers do not fall for it
3.Make sure it does not influence your reputation
4.Will you respond to these activities and how should you inform your consumers?

What to do against phishing?

Nowadays, falling for a phishing email is something that can happen to anyone, as phishing emails get more and more sophisticated. Attackers can access data over the Internet and thousands of phishing messages can be sent in the blink of an eye. To make the messages more convincingly, your brand corporate identity can get abused. By proactively sending information about known attacks using your identity to your consumers, you can prevent them from falling for a certain phishing attempt and phishing attempts alike. However, informing your clients on an ad-hoc basis is no proper education on what to do against phishing, meaning that the awareness amongst your potential victims will dissipate. Therefore, a mixture of both would be perfect. A regular message towards the consumers regarding information how to spot a phishing mail and a direct mail after an incident would be most beneficial.

Informing clients about phishing attempts

Pro-actively informing consumers about relevant phishing attempts is something that must be done if your brand is abused, but what information should you send to your consumers? The information that you should disclose needs to include at least three factors, being; simplicity, transparency and security. Consumers expect a simple solution in an easy to read format. Consumers also demand transparency. Since they are targeted by phishing attacks they should be informed as why they are targeted and how they can secure themselves against these attacks. Finally, consumers require security to ensure trust and provide a level of confidence towards the consumer. Consumers expect that phishing attacks are monitored and that their personal information is secure.

Gathering information about ongoing phishing attempts is key. There are multiple vendors which supply environments which allow companies to keep track of phishing attempts. If an incident is spotted, it is recommended to inform the consumers about this.

A few guidelines on how to inform your customers
The table below depicts a few simple guidelines that might help in creating an email to inform consumers about an on-going phishing attack.

DO	DO NOT
Inform consumers why they are targeted.	Go into details about the impact on your business.
Explain what the purpose of the attackers is.	Get into technical details about botnets, malware, etc.
Present consumers with an example of the phishing email.	Use the actual phishing email.
Point out how the phishing email can be identified.	Use actual phishing links or malicious attachments in your email.
Send an email during a major on-going phishing attempt.	Send an email on every phishing attempt using your brand.
Provide information on how to recognize phishing attempts in the future.	Include links or attachments in your email.
Practice proper cyber hygiene: never ask customers about their sensitive information outside of protected channels and inform them about your policies.	

Contact

Hugo van den Toorn
Consultant - Cyber Risk Services
hvandentoorn@deloitte.nl
+31 (0)88 28 86 238

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.nl/about for a more detailed description of DTTL and its member firms.