

# Cyber Risk Management — Phishing

30 décembre 2016

Recent events (e.g. the cyber-attacks on the Democratic National Committee during the recent United States election) are important reminders of the need for vigilance against **one of the most common and successful kinds of cyber-attacks – phishing**. Organizations should take appropriate technical and administrative precautions to protect against phishing attacks.

## What is Phishing?

Phishing is the use of a fraudulent message that purports to be from a trusted source (e.g. a financial institution, government organization, online service, colleague or friend) designed to cause the recipient to inadvertently disclose sensitive information (e.g. passwords or credit card details) or install malware on their computing device. There are various kinds of phishing. For example:

- "Clone phishing" copies an actual message from a legitimate source but makes slight changes to the message (e.g. changes to embedded links or internet addresses) so that the message has a malicious effect (e.g. installs malware or connects to a spoofed website).
- "Spear phishing" uses a message that contains information specific to the recipient (e.g. information taken from the recipient's social media accounts or business websites) or purports to be from a sender personally known to the recipient (e.g. an executive from the recipient's organization) to gain the recipient's trust.
- "Whaling" is a form of spear phishing directed at a senior executive or other high-profile recipient (i.e. a big fish or whale).

## Why is Phishing a Threat to Organizations?

Phishing is an attack vector designed to facilitate various forms of cybercrime, such as a ransomware attack, hacking to gain unauthorized access to information technology systems and data and financial fraud, which can result in significant loss and liability (e.g. business disruption, financial loss, loss to stakeholder value, reputational harm, trade secret disclosure and other competitive harm, legal noncompliance liability and civil liability to customers, business partners and other persons) to the victim organization and other persons.

Phishing is a serious threat because it works. PhishMe's Enterprise Phishing Susceptibility and Resiliency Report 2016 reported that 91% of cyber-attacks and resulting data breaches begin with a spear phishing email. Verizon's 2016 Data Breach Investigations Report reported that 30% of all targeted recipients opened a phishing message and 12% of recipients clicked on malicious attachments or links that enabled a cyber-attack to succeed.

## **Best Practices/Risk Management**

Managing phishing risk requires an organization-wide, interdisciplinary effort with participation at all levels of an organization (e.g. executives, managers, employees and contract workers from all departments and disciplines). Following is a summary of some recommended practices to protect against and minimize impact of phishing attacks:

- Email Hygiene Technology: An organization should implement and regularly update email filters and anti-phishing software, promptly apply security patches and updates, and implement procedures for monitoring email traffic for suspicious activities.
- Policies/Procedures: An organization should establish, implement and regularly review and update reasonable policies/procedures for the acceptable use of email, messaging and information technology resources and the reporting of suspicious emails and messages.
- Education/Training: An organization should educate and train its personnel (including senior management and directors), during onboarding and at regular intervals afterward, to recognize and report suspicious emails and messages. An organization should consider conducting a phishing simulation as part of its training program.
- Network Structure/Security: An organization should structure its information technology systems, and implement strong security measures and internal access controls, to protect the systems and connected devices from a phishing attack and to minimize the harm/loss that can result from a successful phishing attack.
- Incident Response Plan: An organization should establish a cyber incident response plan that includes procedures and guidelines specific to a phishing attack and should use a testing, training and exercise program to help ensure that the incident response plan is up-to-date and the organization's personnel and information technology systems are in a state of readiness, so that the organization is able to respond to a phishing attack in a timely, effective and lawful manner.

## **Comment**

Phishing attacks are a significant threat to organizations of all kinds, and present risks of significant loss and liability. Organizations should take appropriate precautions to protect against phishing attacks and to minimize the harm resulting from a successful attack.

**Par**

**Services**

[Cybersécurité, respect de la vie privée et protection des renseignements personnels](#)

## BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

[blg.com](http://blg.com)

### Bureaux BLG

#### Calgary

Centennial Place, East Tower  
520 3rd Avenue S.W.  
Calgary, AB, Canada  
T2P 0R3  
  
T 403.232.9500  
F 403.266.1395

#### Ottawa

World Exchange Plaza  
100 Queen Street  
Ottawa, ON, Canada  
K1P 1J9  
  
T 613.237.5160  
F 613.230.8842

#### Vancouver

1200 Waterfront Centre  
200 Burrard Street  
Vancouver, BC, Canada  
V7X 1T2  
  
T 604.687.5744  
F 604.687.1415

#### Montréal

1000, rue De La Gauchetière Ouest  
Suite 900  
Montréal, QC, Canada  
H3B 5H4  
  
T 514.954.2555  
F 514.879.9015

#### Toronto

Bay Adelaide Centre, East Tower  
22 Adelaide Street West  
Toronto, ON, Canada  
M5H 4E3  
  
T 416.367.6000  
F 416.367.6749

Les présents renseignements sont de nature générale et ne sauraient constituer un avis juridique, ni un énoncé complet de la législation pertinente, ni un avis sur un quelconque sujet. Personne ne devrait agir ou s'abstenir d'agir sur la foi de ceux-ci sans procéder à un examen approfondi du droit après avoir soupesé les faits d'une situation précise. Nous vous recommandons de consulter votre conseiller juridique si vous avez des questions ou des préoccupations particulières. BLG ne garantit aucunement que la teneur de cette publication est exacte, à jour ou complète. Aucune partie de cette publication ne peut être reproduite sans l'autorisation écrite de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Si BLG vous a envoyé cette publication et que vous ne souhaitez plus la recevoir, vous pouvez demander à faire supprimer vos coordonnées de nos listes d'envoi en communiquant avec nous par courriel à [desabonnement@blg.com](mailto:desabonnement@blg.com) ou en modifiant vos préférences d'abonnement dans [blg.com/fr/about-us/subscribe](http://blg.com/fr/about-us/subscribe). Si vous pensez avoir reçu le présent message par erreur, veuillez nous écrire à [communications@blg.com](mailto:communications@blg.com). Pour consulter la politique de confidentialité de BLG relativement aux publications, rendez-vous sur [blg.com/fr/ProtectionDesRenseignementsPersonnels](http://blg.com/fr/ProtectionDesRenseignementsPersonnels).

© 2025 Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Borden Ladner Gervais est une société à responsabilité limitée de l'Ontario.