webnames
CORPORATE

PHISHING & BUSINESS EMAIL COMPROMISE

HOW CANADIAN BUSINESSES SHOULD BE PROTECTING THEMSELVES GOING INTO 2018

The numbers are startling. Canadian businesses are losing over $3 billion dollars annually to cybercrime, and experienced a reported average of 44 cyberattacks per year in 2016.

While most Canadian businesses are acutely aware that cyberattacks are increasing in frequency and sophistication, the majority are falling behind when it comes to evolving their detection and prevention strategies. In fact, it's estimated that only 43% of Canadian businesses are presently able to detect a sophisticated attack.[1]

In another striking finding, the Canadian Securities Administrators (CSA) in their survey of 1000 firms, found that phishing, including spear phishing, and impersonation via fraudulent emails, ranked as the first and third most common cyber incidents experienced[2]. That's right, plain old email is still arguably the weakest link in cyber threat prevention and the most frequent point of entry for corporate infiltration.

In the rush to conduct risk assessments and revamp security frameworks, it's unfortunately not uncommon for basic preventative measures to get overlooked. One important example of this type of oversight is in how an organization's internal information can become publicly accessible on the Internet, as a result be leveraged by bad actors. This vulnerability extends into how an organization implements their domain management strategy in partnership with their domain name registrar.

While high-profile ransomware incidents such as the WannaCry and NotPetya outbreaks have grabbed the headlines this year, according to Cisco's mid-year security report, phishing, spear phishing and compromised email passwords represent a much bigger financial threat to organizations. Phishing, and more specifically, business email compromise (also known as BEC) attacks rose by 45% in the last three months of 2016 over the three months previous.

---

[1] Canadian Businesses Lose Billions of Dollars to Cyber Crime Each Year - Canadian Chamber of Commerce, March 2017 &The Cyber Security Readiness of Canadian Organizations - 2017 Scalar Security Report 2017, February 2017

[2] Cybersecurity Risks—Compelling Statistics from the Canadian Securities Administrators - BennettJones.com, October 2017

The seriousness of this threat led to US Homeland Security Chief Jeh Johnson calling phishing the agency's "top hacking threat" back in November 2016. Johnson, addressing a crowd of cyber security and law enforcement professionals, noted that "the most devastating attacks, by the most sophisticated attackers, almost always begin with the simple act of spear-phishing."

For those who are unaware of the differences, let's review the most common phishing attacks facing businesses today.

THE MANY FACES OF PHISHING & BUSINESS EMAIL COMPROMISE

With a standard phishing attack, a generic message is typically sent to large groups of people, sometimes in the same organization. Fraudsters may impersonate a legitimate company (UPS, PayPal, major banking institution, etc.) by creating official looking correspondence in an attempt to steal personal or corporate information or install malware.

Spear phishing attacks, in contrast, tend to be well crafted, targeted and personalized. Cybercriminals will research their targets, creating highly customized emails that can include multiple sources of information such as the recipient's name, job title, location, and even reference friends or business contacts. Emails can appear to come from a trusted source such as a vendor, organization or social media website that the victim has a relationship with.

Executive Whaling or **CEO Fraud** is another breed of spear phishing that specifically targets corporate executives or administrators. Again, substantial research can go into these attacks, with the aim of gaining access to an executive's email to steal information or target other employees in financial positions who have the authority to move money.

Of the above, spear phishing is the most frequently used variant in business email compromise. Financial losses attributed to BEC grew by 2370% in the US between January 2015 and December 2016[3] , and has evolved from bad actors masquerading as c-suite executives requesting wire transfers, to bad actors meticulously impersonating known suppliers or vendors and requesting payment of invoice. Targets of BEC can be anyone with credentials to conduct payments or authorize a transfer of funds — the money ending up in accounts controlled by individual cyber criminals or increasingly, criminal organizations. Businesses of all sizes, not-for-profit organizations, academic institutions and government are all vulnerable to these scams.

In a recent close-to-home example, Alberta's MacEwan University was defrauded of $11.8 million when staff sent direct payments to accounts set up by cybercriminals who impersonated one of the institution's major vendors, a local construction company with whom they had a 10 year business relationship. Then there was the revelation back in April that both Google and Facebook were defrauded of over $100-million by a Lithuanian man who impersonated a Taiwanese electronics manufacturer, forging email addresses, invoices and contracts by using the names of company executives.

[3] Business Email Compromise :The 5 Billion Dollar Scam – Federal Bureau of Investigation, May 2017

PREVENTATIVE MEASURES TO REDUCE PHISHING AND BEC VICTIMIZATION

The good news is there are many simple and highly effective measures that organizations can implement to protect themselves and reduce the likelihood of being victimized by phishing and BEC attacks.

Some core safeguards include:

- Ongoing employee training about how to identify spoofing;
- Establishing strong protocols and procedures (e.g., a shortlist of authorized employees with permission to approve and process payments; multi-factor authentication and in-person or phone approvals for sending money; daily withdrawal limits, etc.).
- Implementing technology solutions to identify malware, keystroke logging and email spoofing.

Another extremely important line of defense for organizations, and one does not get the attention it deserves, is the management of private corporate information and the contact and/or personal details of c-suite and high-level executives.

Limiting the amount of information that is available online and that can be used for impersonation, spoofing, and in the contact information of look-alike domain registrations is a critical protective measure that requires a systematic, procedural approach and one that extends to the registration and management of a company's domain names.

The **WHOIS database** is an online repository of information that is collected when domain names are registered. It stores and publicly displays information such as domain creation and expiry dates, the registrar of record (e.g. Webnames.ca), and the name, address, phone number and email of a domain's registrant, billing, administrative and technical contacts. Because the WHOIS is an open and public entity, it is also widely exploited - the contact information it contains is actively mined and harvested for use in a wide variety of criminal activities, including harassment, spam generation, identity theft and phishing, among other cybercrimes.

When the names and contact information of executives, marketing, legal or IT personnel are available in the public WHOIS record of a domain name, you increase the risk of your brand being impersonated to carry out spear phishing or BEC activities, and of being attacked yourself by publicly exposing personnel that can be targeted or used as points of infiltration. Information mined from the WHOIS may also be used in conjunction with information combed from social networks, among other sources, to build mirror personas to attempt to wrest access and control over external accounts or business critical services.

Do you know what information is listed in the WHOIS record of your domain names?

Click here to find out.

With Symantec's 2017 Internet Security Threat Report revealing that one in approximately every 2500 emails is a phishing scam and that more than 400 businesses face a BEC[4] attack each day , first line of defense measures such as domain name privacy are extremely important with an organization's overall security framework.

Utilizing a WHOIS service such as Webnames Privacy that substitutes non-personally identifiable information in place of corporate information (e.g., contact names, email addresses, phone numbers, etc.) to effectively anonymize a domain's WHOIS record eliminates the risk that your information will be scraped from the WHOIS and then used for nefarious purposes.

[4] Internet security Threat Report, Volume 22 – Symantec, April 2017

It's important that organizations take proactive and layered measures to prevent phishing because the consequences extend beyond financial fraud and compromised network security. Organizations that fall victim to phishing, either by being defrauded or being impersonated, can also experience damaging residual impacts such as brand erosion, reputational harm, loss of trust and loss of business.

CONCLUSION

In addition to ongoing employee education, protective protocols and defensive technologies such as antivirus and malware protections, organizations must better manage and control the information they publish on the Internet. Designating "safe" contact information, using it consistently, and closing the loop on vulnerabilities such as WHOIS information can help to limit an organization's susceptibility to identity theft, phishing and business email compromise. And while no single or combination of counter measures can completely guarantee protection, there are numerous simple and low-cost measures that can powerfully reduce the threat.

To request a complementary WHOIS privacy audit on your domain portfolio, or a more comprehensive security review to identify the domain security measures your business should be using, please contact Webnames Corporate Services.

Webnames Corporate Services

Suite 333 - 333 Terminal Avenue
Vancouver, BC V6A 4C1
Toll Free 1 866 470 6820
Email: corporate@webnames.ca
Website: corporate.webnames.ca