HACKED:
Small Businesses in the Crosshairs
The Small Business Threat Onslaught and How to Shield Against It

Introduction

Cyberattacks continue to escalate every day – threatening businesses worldwide.

While large corporate victims of cyberattacks may suffer financial losses and reputational damage, most eventually bounce back. However, for smaller businesses with limited resources, bouncing back is easier said than done—especially considering the average costs of an attack:

USD 20,752

per threat for some small businesses .[1]

USD 879,582

spent by SMBs to repair damage or address data theft .[2]

These costs could break many small businesses. And the common culprit for 90 percent of network security breaches is spear-phishing.[3] Unfortunately, these threats are only becoming more pervasive, with 55 percent of small businesses reporting a cyberattack in the past 12 months.[4] And in the past year alone, ransomware rose by 250 percent[5] and business email compromise/email account compromise (BEC/EAC) scams are up a staggering 2,370 percent.[6]

At PhishMe, we believe that all businesses – regardless of their size – should be able to protect against the impact of phishing attacks. This white paper was written to help you do just that.

Limited Resources Entice Criminals

Threat actors like smaller companies because they typically have fewer resources than their corporate counterparts to fend off attacks.

10% of small businesses surveyed had a separate budget for cybersecurity.[7]

61% said cybersecurity was just a part of their IT departments.[8]

Small businesses also tend to have smaller IT teams, which, for cybercriminals means less obstacles. And easy entry via phishing emails lets criminals collect data or steal funds over extended periods of time.

In fact, hackers dwelled in the network belonging to General Linens Service, Inc for two years before they were discovered, according to Symantec's "2016 Internet Security Threat Report."[9]

“Awareness” Does Not Mean ”Prepared”

A recent ransomware survey by the Ponemon Institute revealed that small businesses have conflicting perceptions about the threat:

57% of those surveyed thought their company was too small to be a target of ransomware.[10]

51% said their company had actually experienced a ransomware attack.[11]

46% believe the prevention of ransomware attacks was a high priority for their company.[12]

So while SMBs believe they are too small or insignificant for ransomware attacks, many have already been attacked and believe prevention is a company priority.

Adding to the complexity, limited or non-existent resources underlie the challenges of educating and protecting the organization from phishing emails. Too often, long-term security planning and training falls by the wayside leaving many small businesses unprepared for the unavoidable attacks.

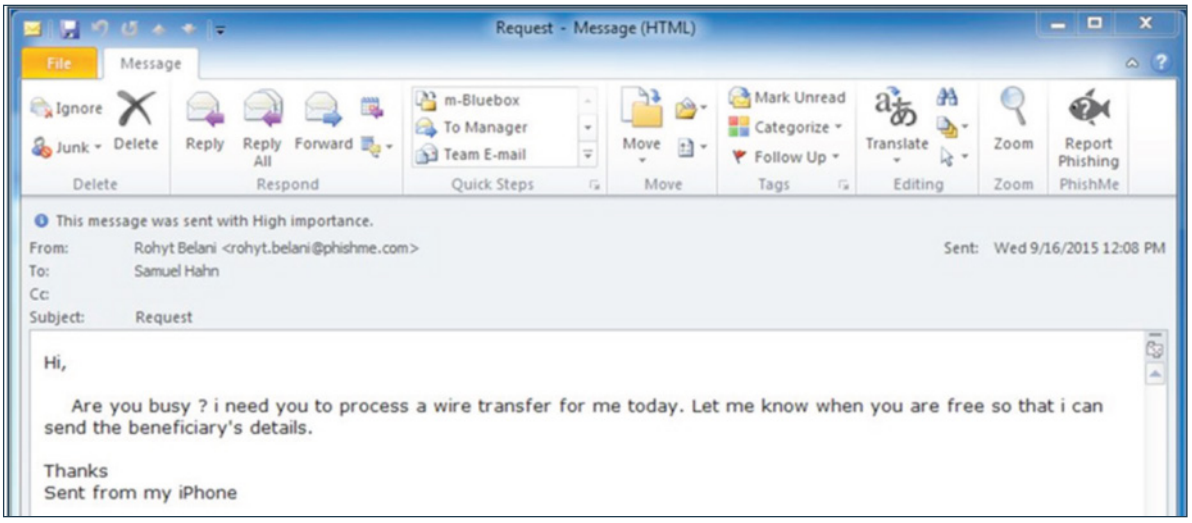
9% felt their company was “extremely well-positioned” to respond to a security threat.[13]

66% ranked ransomware as a dangerous threat, but only 13 percent gave their company a high rating for preparedness.[14]

CASE STUDY: No One is Safe – Not Even PhishMe

It’s strange that someone would try to phish PhishMe, the leader of anti-phishing solutions. But it proves that no business is immune to the threat - regardless of industry or size.

When phishers first targeted PhishMe with a business email compromise email on Sept. 16, 2015, they impersonated Rohyt Belani, PhishMe Co-founder and CEO, in an email to Sam Hahn, PhishMe Vice President of Finance. This screenshot shows how clever scammers tried to open the door to extort money from us.



Because Sam (and all our employees) participates in the PhishMe simulation program, he knew how to identify this email as a phishing threat. The key to thwarting this attack was simple - conditioning to look for and recognize the signs of phishing. In this case, it was the signature that gave it away. Rohyt does not use an iPhone.

> "If PhishMe can help us defend against potential data breaches, and help us keep the lights on and the natural gas flowing for our customers, that's a big deal"
>
> **— Cybersecurity Awareness Manager, $30B U.S. Energy Company**

How to Shield Against Cyberthreats

PhishMe's experiences as a target make us even more determined to help other businesses avoid the damage caused by phishing emails. When your small business gets attacked, will you be prepared? Here are some ways to prevent and respond effectively to cyberattacks and phishing threats:

1. Establish a limited, basic security program, focused on the biggest risks and simplest processes.
2. Back up all data frequently and completely. It's one way to possibly avoid paying ransom in the event of a ransomware attack.
3. Identify potential attacks that would have the greatest impact and protect those assets.
   - Ransomware – If your biggest concern is that your access to patient files or business data will be blocked, focus on what you can do to protect those assets in the event of a ransomware attack.
   - Threats to products and services – If you provide goods or services, put together contingency plans that will combat disruptions to service and product sales.
4. Adopt a comprehensive antiphishing program that empowers all your employees to act as the last line of defense against threats that bypass other security solutions. This is crucial, as 90% of network security breaches begin with phishing.[15] Your antiphishng program should include:
   - Periodic, relevant phishing simulations to familiarize and educate employees as to how phishing messages look, act and sound.
   - A reporting process to actively engage employees in your security efforts.
5. If you already use a phishing simulation program:
   - Create examples of real-world phishing threats that your company receives and add them to your phishing simulation rotation.
   - Provide enough opportunity for education and reflection – simulations should be run periodically as part of an overall program.
6. Leverage additional resources. There are many free and low cost resources avaiable online including:
   - PhishMe CBFree - 18 Security Awareness CBTs available in 8 languages
   - PhishMe Free - A free simulation tool available for companies under 500 employees.
7. Increase security spending – if possible.

> “Our PhishMe program gave us valuable information that we could use immediately to target our efforts to improve our defenses”
>
> **— Chief Information Security Officer, $10B Regional U.S. Bank**

Conclusion

As small businesses grow in number, and prominence, they will become even bigger targets for criminals. Like large corporations, they need to prepare.

All businesses should have the awareness and basic tools to fight back.

With 90 percent of network security breaches beginning with phishing,[16] it’s critical to empower your employees to recognize and respond to phishing threats.

NEXT STEPS

Learn more, and sign up for PhishMe Free. Start building your own human firewall against phishing attacks.

---

1 National Small Business Association, “2014 Year-End Economic Report,” 2014.

2 Ponemon Institute, “2016 State of Cybersecurity in Small and Medium-Sized Business,” June 2016.

3 PhishMe, “Enterprise Susceptibility and Resiliency Report,” 2016.

4 Ponemon Institute, “2016 State of Cybersecurity in Small and Medium-Sized Business,” June 2016.

5 Kaspersky Lab, “Kaspersky Lab Quarterly Malware Report: IT threat evolution Q1 2017. Statistics,” May 22, 2017.

6 * FBI, “Business Email Compromise Email Account Compromise: The 5 Billion Dollar Scam,” May 4, 2017.

7 The National Center for The Middle Market, “Cybersecurity and the Middle Market, The Importance of Cybersecurity and How Middle Market Companies Manage Cyber Risks,” 2016.

8 Ibid.

9 Symantec, “Internet Security Threat Report,” April 2016, Volume 21.

10 The Ponemon Institute, The Rise of Ransomware, January 2017.

11 Ibid.

12 Ibid.

13 The Hartford and Advisen, “Cybersecurity Preparedness and Response a Middle Market Risk Management Perspective,” 2015.

14 Ibid.

15 PhishMe, “Enterprise Susceptibility and Resiliency Report,” 2016.

16 Ibid.

PHISHME

For more information contact:

W: phishme.com/contact T: 703.652.0717

A: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175