Best Practices for Protecting Your Small or Medium Size Business from Phishing

DuoCircle

www.**duocircle**.com

Table of Contents

A problem that can't be **solved** (completely)

If you're responsible for IT at a small or medium size business, you understand the threat from phishing and other email-based attacks. More than 90% of all cyber-attacks begin with a phishing email. It explains why less than half of IT executives surveyed believe their ability to block phishing attempts from their users is effective, according to research conducted by Osterman.

When you realize that the threat from phishing is partly technology and partly human nature, then you also understand that it's not something you fix once and forget. You're never 100% protected because attackers never stop evolving and developing new techniques and varying their approaches. A sophisticated cyber-attack always has the potential to penetrate even the best cyber defenses.

When it comes to protecting your company from phishing, malware and spoofing, it's less about trying to solve the problem completely and more about mitigating and managing your risk continuously.

It's about mitigation

Mitigating the phishing problem requires taking a holistic approach. For a small business that means combining phishing awareness training and technology for protection because training alone has proven to be ineffective as a long term strategy.

On the technology side it means combining on-premise with cloud-based solutions. But mostly what it means is taking a layered approach to email defense because no single piece of hardware, software or training effort will protect your users.

A layered approach, which is almost always employed in large organizations, has been unaffordable for smaller businesses until recently. And while it may seem counterintuitive, the layered approach is essential for those using hosted email services like Office 365. That's because native security solutions in hosted services are often inadequate. They present a large attack vector that's hard to defend. And because it's just not their core expertise.

Hosted solutions are generally less capable of defending against exploits called zero-day vulnerabilities. One of the latest and most damaging malware variants is an Office 365-based zero-day exploit called baseStriker. Cybercriminals took advantage of a flaw in the way Office 365 servers qualify incoming emails to send malicious code through a rarely-used HTML tag that Office 365 doesn't support or recognize.

Whether you use an on-premise or a hosted email solution, one of the simplest and most effective mitigation techniques to fight phishing is not to allow such email onto your network in the first place.

76% of businesses reported being a victim of a phishing attack in the last year

- Wombat

Training alone won't do it

Training is essential but...

Training employees to raise awareness of phishing attacks is an major component in an overall security strategy, but it's not the most important one. If you're budget limited and can only afford to do one thing, then prevention technology should come first.

Why? Because even the best security training isn't 100% effective. And because it only takes one employee to click on one malicious link and the whole network could be compromised.

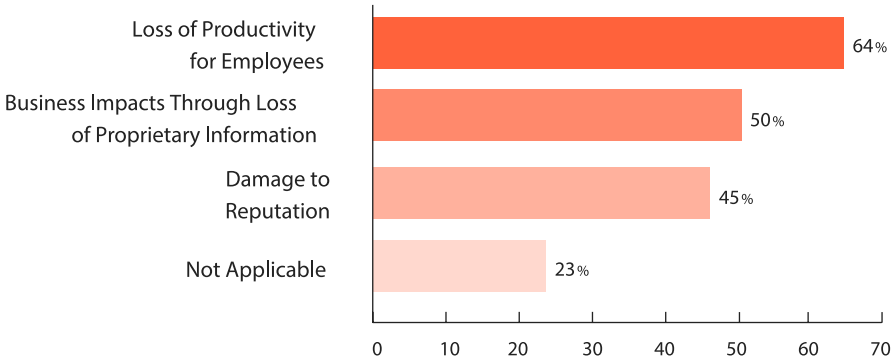
Despite years of corporate education, phishing still remains the single most successful means of illicitly gaining access to business assets. People may be aware of the fact that an email could be suspicious, but that doesn't keep some of them from clicking it. Curiously some of the worst offenders are in the IT department, which is staffed by those who should know better.

Your employees know not to click on executable files but you still install antivirus software. It's the same reason you prioritize phishing prevention technology over training.

Stop threats before they reach your inbox

The best way to stop threats before they reach your company's inbox is to inspect the emails before they reach your company's perimeter. Cloud-based email protection solutions provide a buffer before emails reach your corporate network or your hosted email service.

How do you measure the cost of phishing?



Your confidential corporate information is secured because your employees are simply prevented from visiting sites that misuse such information.

Phishing is a two way problem

Protecting your users and your reputation

Most people in IT think phishing is a one-way problem. Stop threatening emails from reaching your employees and you've solved your phishing problem. But that just isn't true. There is another vulnerability to phishing. And it's one that can cost you your business reputation..

If you're not using authenticated emails, your domain could be used against you. It's called spoofing and attackers could use your domain to phish your customers. And whether intentional or not, the blame would land on you.

When it comes to phishing protection, you need to protect your employees and your customers.

Domain name spoofing protection

Any phishing solution you deploy should protect you and your customers from domain name spoofing. The best way to do that is by sending cryptographically signed emails from an authenticated email server.

There are few methods to authenticate email servers. These include DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework), often in conjunction with DMARC (Domain-based Message Authentication, Reporting and Conformance).

Protect your customers. Authenticate your domains and send cryptographically-signed emails so when they receive your message they'll know it hasn't been tampered with, which means they cannot get phished by domains you control.

More than just checking the email

Checking the email is just the starting point

The starting point for any good anti-phishing technology is link click protection. Any time an email contains an embedded link, it should be checked against multiple URL databases which contain whitelisted and blacklisted websites. In the event a site is marked unsafe, users should be prompted with a warning that they are going to an unsafe website and they should be prevented from opening the malicious links.

In addition to link checking, the headers, the domain information and the body content should also be scanned for inconsistencies. Suspicious messages and payloads should be quarantined as spam, tagged or simply rejected before making it to the user's inbox.

But checking the formatting and content of an email itself is just the starting point. Thorough phishing prevention goes a step further and checks the linked-to website itself. That's because a link that shows up good could point to a malicious website.

Real time website scanning

A good solution should ensure that linked-to websites are scanned for

- page size,
- domain name,
- on-page content, as well as
- hidden fields and
- JavaScript with injection code.

The information should be used to develop a decisioning score as to how likely those elements are to be representative of a malicious website.

The websites should also be compared to Fortune 5000 websites, bank websites and other frequently-used websites. The should be checked to ensure that elements have not been copied to look like clones of authentic sites. Even SSL certificates are no longer a good indicator of a site's security. Reputations for the senders, the domain and the site content have to be evaluated in real time, when the linked is clicked, not just when the email first arrives in the inbox.

If it isn't real time don't bother

Do you know that most phishing domains are live and active for less than 36 hours? That's right. If you're anti-phishing solution checks URL databases every 24 hours, the chances are it will miss the threat window completely. If you're phishing solution isn't checking databases in real time, every few minutes or so, you may as well not bother.

> Effective phishing mitigation is about timing.

Continuous link checking

Real time or near real time link checking is essential to combating phishing attacks. The link can't just be checked for emails upon arrival. It must also be checked after the email arrives, when the link is actually clicked. Every time it's clicked.

One of the more sophisticated techniques of ransomware, Cryptolocker, is a scheme in which the attackers send an email from a domain or a URL with a good reputation. When the emails are delivered the site is clean, but within a few hours the hackers switch out the safe content on the site for their harmful payload.

The only way to defend against these time-delayed activation techniques is to automatically check every clicked link in every email against multiple URL reputation databases, every time the link is clicked.

Post-delivery protection is essential. Your emails must be protected from harmful clicks in real time.

Notifications should also be in real time

Link checking isn't the only thing that should happen in real time. Users should get instant feedback in the form of an alert when a suspicious link is about to be visited. Each time a user clicks on a suspicious link, the user and the system administrator should be alerted to the malicious link immediately.

By providing instant feedback to users about the threats associated with such links, not only are employees protected, but they gain a higher level of awareness. Real time alerts provide a learning reinforcement opportunity to improve their ability to assess the risks of such email threats in the future.

30% of phishing messages get opened by targeted users

- Verizon

A holistic approach to phishing mitigation

Your approach to phishing protection should be a holistic one. It should accommodate on-premise as well as hosted email systems. It should provide protection for all devices, offer settings you control and have a simple user interface where administrators can see and control the entire situation from a single pane of glass. And it should also include a layered approach to security.

A layered approach

A layered approach to anti-phishing protection provides a series of safeguards. Like a succession of hurdles in a row. With each additional hurdle making it less and less likely that a malicious email gets through.

Even with a hosted email solution, it's wise to augment it with a cloud-based service provider as it provides an additional layer of defense. And cloud-based service providers can be more effective at protecting against zero-day exploits because they continually feed the data they uncover back to the list and data providers in real time. This positive feedback loop makes cloud service providers quicker at detecting new threats and outbreaks.

Protection for all devices

Handheld and mobile devices are a way of life in business today. Your phishing protection solution should account for that. But you shouldn't have to install a new plug in or configure software every time an employee changes machines or brings in a new device.

The simplest way to become device independent and alleviate the need for custom software configuration is to protect the device before the email gets to the device. Email security solutions that are outside your corporate network give you the flexibility to provide protection for all your devices without having to accommodate for changing devices.

Protection with settings you control

Your email protection solution should offer you more than just an on and off switch. Every company has its own set of rules and exceptions and how they want things configured. You should be able to tweak and tune the criteria used to filter your emails. You should have the ability to access logs to understand your threat environment. At the very least you should have the ability to customize your whitelists and blacklists.

Simple dashboard control

Your email protection solution should offer you complete situational awareness and control of your system from a single unified web-based console. The console should include access to activity logs and provide a real time view into the email queue. And all configurations and services should be controllable from the console.

Price and convenience matter too

Email protection doesn't have to be expensive or difficult

Email protection started as an enterprise solution with enterprise prices for enterprise clients. The problem is that level of protection never made it to small and medium size businesses (SMB) at a price they could afford. To make matters worse, it hasn't always been easy for SMBs to obtain that kind of advanced protection. From challenging integrations to a lengthy sales process to three year contract commitments.

As an SMB, you should look for a service provider who makes email protection fast, easy and affordable. No sales calls. No contracts. Up and running in ten minutes.

You should also look for a provider who doesn't charge a per user fee, but rather charges a fixed fee for a given level of service, so you can better control your expenses. This is especially true for large groups that communicate infrequently via email like alumni associations. There's no reason you have to pay a per user fee if you only have a handful of employees.

Summary of best practices

Below is a list summarizing the best practices covered in this post for protecting your small or medium size business from phishing attacks.

1. 

Understand that thwarting phishing attacks is not a one-stop solution and requires continuous mitigation.

2. 

Training is an essential part of an overall security strategy but if you only have a limited budget, spend it on phishing prevention technology.

3. 

The single best way to stop threats before they reach your employee's inbox is to inspect the emails before they reach your company's perimeter by using a cloud-based email service to act as a buffer.

4. 

In addition to inbound phishing protection, you also need domain name spoofing protection to shield your reputation.

5. 

Email protection should take a holistic and layered approach to mitigation.

6

Anti-phishing technology should check more than just embedded email links.

7

Anti-phishing technology should conduct all checks in real time as well as provide alerts in real time.

8

Email protection should provide protection for all devices.

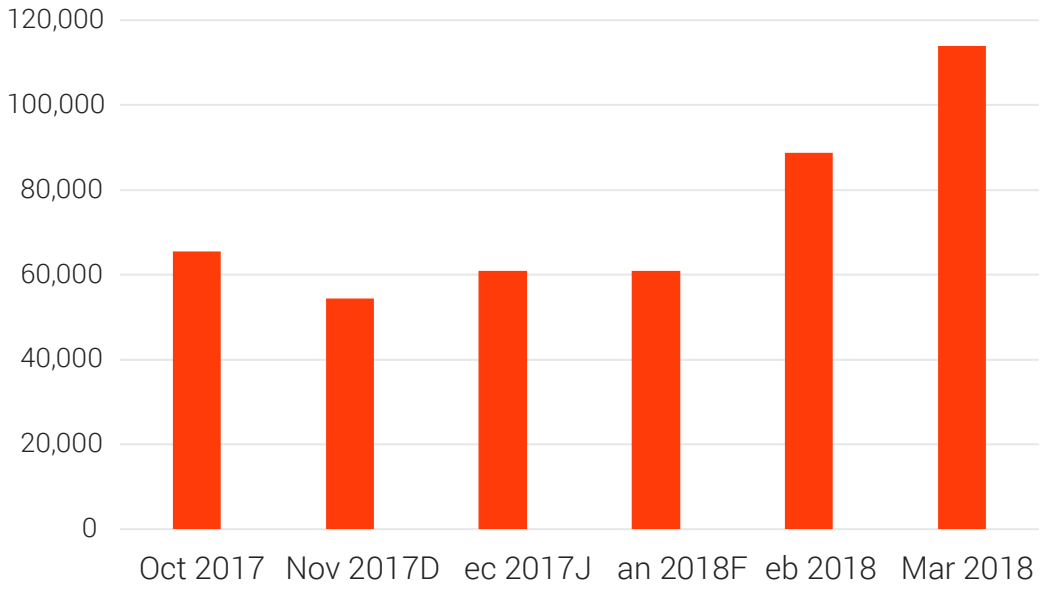
9

All email protection should be administered from a single web console and provide settings you control.

10

There is no reason for a small or medium size business to pay enterprise prices and be locked into enterprise contracts for anti-phishing service.

Unique Phishing Sites Detected,
4Q2017-1Q2018



Conclusion

Whether it's email phishing, spear phishing, and whaling attacks, malicious emails are not going away. You know you need to protect your employees, your data and your customers. The challenge is to do it effectively, with as little interruption to your business as possible, and at price that fits your budget.

In this post we have covered ten best practices you can start implementing immediately. When it comes to protecting your SMB against email attacks, an investment in anti-phishing technology does fall under the category of an ounce of prevention. Isn't it time to make that investment?

95% of all attacks on enterprise networks are the result of successful spear phishing

- SANS Institute

DuoCircle

If you want to learn more

Visit our Website

Contact Us

www.**duocircle**.com

support@**duocircle.com**

(+1) **855-700-1386**

Keep up with our Social Media at:


/duocirclellc


@duocirclellc


DuoCircle