

HARPOONING EXECUTIVES

How phishing evolved into the C-suite

TABLE OF CONTENTS



<input type="checkbox"/>	FW: Top 4 IT Providers	Mishelle Porter	3/24
<input type="checkbox"/>	FREE BUY FREE BUY...		3/24
<input type="checkbox"/>	Webinar: Spam Protect..	Cloud Solutions Inc.	3/23
<input type="checkbox"/>	Delivery: Track Package	Kole Keaton Shipping	3/22
<input type="checkbox"/>	Re: Yearly Sales Goals	Ashley Carter	3/20
<input type="checkbox"/>	Get your IT essentials...	Best IT Provider Inc.	3/20
<input type="checkbox"/>	Monthly AP Reports	Troy L. Willis	01.05

The whalers who scammed \$17 million	4
Partner interview with Alex Markov, President Red Key Solutions	8
In the beginning it was relatively harmless: Pushing products to the masses	12
Phishing: How criminals made you their product	14
Spear phishing: When criminals have a target in mind	18
Whaling: When spear phishing harpoons the biggest fish	22
Interview with Jonathan Levine, CTO Intermedia	24
How to protect yourself	28
Educate your users and executives	
Install comprehensive protection & protect your “attack surface”	
Prepare for the worst	
Partner interview with Bart McDonough, CEO Agio	42
Conclusion	45
Intermedia Hosted Exchange	
Intermedia AppID® for single sign-on	
Intermedia SecuriSync® for secure file sync and share	
Intermedia Email Archiving	
McAfee Advanced Protection with ClickProtect	
McAfee Data Loss Prevention	
About Intermedia	49
About Intel Security	49

THE WHALERS WHO SCAMMED \$17 MILLION



80% FAILED TO SPOT
ONE phishing
email

Source: Phishing Deceives the Masses: Lessons Learned from a Global Assessment, McAfee

In June 2014, Keith McMurtry, financial corporate controller for Scoular Co. lost \$17 million of the company's money. And it all started with an email.

Scoular Co. is ranked 55th on Forbes' 2014 list of America's Largest Private Companies with \$6.2 billion in annual revenues. On June 26, 2014 someone decided they wanted a share of those revenues.

Keith McMurtry was sent a seemingly innocent email from Scoular's CEO, Chuck Elsea. This email asked McMurtry to wire \$780,000, to a bank account in China.

"I need you to take care of this," read the email from the attackers pretending to be Elsea. "For the last months we have been working, in coordination and under the supervision of the SEC, on acquiring a Chinese company... This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations."¹

This didn't raise any concerns for McMurtry as he knew about the acquisition plans. And although the email didn't come from Elsea's corporate email account, McMurtry knew he was traveling and Scoular's accounting firm had been copied. McMurtry transferred the money.

The next day a second email was purportedly sent from Elsea instructing McMurtry to contact a specific employee of Scoular's accounting firm for additional details on where to wire the next batch of money. McMurtry called the number provided and spoke to this employee about the deal. So when the email from the accounting firm arrived instructing him to wire \$7 million to Shanghai Pudong Development Bank, he did so without question.

The last email was sent three days later instructing him to wire an additional \$9.4 million to the bank. McMurtry again complied. A few days later it was discovered this was all a complicated email phishing scam. In less than a week, Scoular Co had lost \$17.2 million to a "whaling" attack, unlikely to ever be recovered.

It's the ultimate cautionary tale: whaling can cost companies millions. And sadly this isn't the only story out there. Many recent headlines show how prevalent these attacks have become.

THIS THEN RAISES THE QUESTION: COULD THIS HAPPEN TO YOUR COMPANY? THE SHORT ANSWER IS YES.

There are



**things you can do to
counteract this threat**

1.

Educate your users & executives

Phishing is effective because people trust their company email and assume that its security technology will catch all threats. But technology is only one aspect of defense. Educating users on the dangers of phishing can raise awareness with employees so they are on alert and think twice before clicking links or opening an email attachment.

2.

Deploy comprehensive protection and protect your “attack surface”

Technology offers a first layer of protection to assist employees in making the most security-conscious decisions. Deploying anti-malware filters, from industry leaders like Intel Security, can help prevent malicious emails from making their way into users’ inboxes. Other technology such as real-time URL scanning can offer a second layer of defense if malicious mail evades malware filters and a user clicks a link. Finally, take a hard look at the email addresses that can receive email from the outside world. Each one represents a hole in your “attack surface” and a potential way for phishing emails to get in.

3.

Plan for the worst case scenario.

Even with all the technology and awareness safeguards in place, the rapid evolution of phishing techniques makes it nearly impossible to protect companies from 100 percent of threats. You must prepare for the worst and enable additional safety measures to greatly reduce the potential impact of an attack.

THIS EBOOK WILL EXPLORE ALL THREE RECOMMENDATIONS. BUT BEFORE YOU CAN SOLVE THE PROBLEM, YOU HAVE TO CLEARLY UNDERSTAND IT.

Partner Interview with Alex Markov

President, Red Key Solutions

WHAT TYPES OF PHISHING HORROR STORIES HAVE YOU SEEN OR HEARD AMONG THE COMPANIES THAT YOU WORK WITH?

Before we put McAfee security in place, we saw two terrible targeted attacks. The phishers had obviously done their homework on LinkedIn because they found out who the owner was and who the controller/CFO was, and they spoofed the owner's email. Then they emailed the controller requesting a wire transfers based on properties that they've purchased. Both times the controller fell for it and wired money. And both times it was stopped by the bank. The last time was \$78,000, and the time before that was \$86,000.

We're telling clients to put stop gaps in place on wire transfers because of how sophisticated the attacks have gotten.

HOW DO YOU HELP YOUR CUSTOMERS PREVENT PHISHING ATTACKS?

We stand with our clients like an IT department and we're very vigilant with a high attention to detail. We tell all our clients to send us emails that they're not sure about so we can act as a kind of human filter. And we've also added different technology layers, like DNS level scanning and McAfee spam filtering, and several others which has been given our clients comprehensive all around security.

We also do a user education. We have found that, all the technology in the world, won't help if you are not educated about what to look for.

WHAT TYPE OF PREVENTATIVE METHODS DO YOU PUT IN PLACE?

There are a number of things we do. From a high level, we partner with a company that does security penetration testing and we have a technology assessment that we run on clients which helps us identify any security gaps. If clients are missing antivirus, Windows updates, Adobe updates, firewall rules, Java updates, spam filtering, or email protection we can identify that and ensure they have a roadmap in place to get secure. When our client networks are tight and secure, it dramatically reduces risks.

More strategically, we train new employees that get hired by our clients about email security and link safety. Even the best antivirus in the world won't catch a virus that is a new breed because the technology needs additional time to catch up. So, we focus on teaching our customers to be very skeptical and vigilant about their email and their interactions in the digital world.

WHAT ADVICE DO YOU HAVE FOR BUSINESSES, CLIENTS OR OTHERWISE, TO PROTECT AGAINST THE POTENTIAL RISK OF A CYBER ATTACK?

Number one is have a good IT management firm standing with you. Having an internal IT department may not be enough to get the exposure into the entire technology landscape like an IT management company. It is very important to have a very solid IT partner that can help guide companies through the oceans of the current digital world. Picking the right clouds, picking the right software, picking the right security solutions, balancing usability and security are all problems facing businesses today. An IT management firm can truly help piece all of that together.

Then the second thing I would say is invest properly in technology. Every single time I've seen people under invest it comes back to bite them. The most expensive thing in companies right now is people and payroll. If you're under investing in security and your employees are wasting time on technology issues, then it's a hindrance to the company. Technology becomes an anchor instead of a competitive advantage.

The third thing is educate on how to use technology and what security risks to look for. Once is not enough. You need to continue educating staff consistently. If you educate people that will make the entire workforce more successful and more productive and you will reduce risk.

WHAT ARE SOME RED FLAGS BUSINESSES SHOULD LOOK OUT FOR?

The easiest way to find out if something is a scam via email is to hover your mouse over the link. If you see that the link is not going to a real domain then it's an email trying to steal something.

The second thing is, if you're not expecting it, like a tracking number or airline ticket or something like that, don't fall for it. They're very convincing. We're a LogMeIn customer, and I got an email the other day saying, "Your LogMeIn account was just billed for \$800.00. Please click here to get the invoice." And it looked just like the LogMeIn email. But it was a way to steal LogMeIn accounts, which is ridiculous. So, I would say if you're not expecting it, don't fall for it.

If you are not sure what something is, go to the website directly or call a phone number that you know is real such as a number on the back of your credit card.

: Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give me your current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well Hey Neil, it's Michelle here, it has been a long time huh ? how're you doing ? how's your work with Return Path ? Is everything ok at Epsilon ? Hey, can you believe it! I got married to Brian ! Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give me your current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well, here I'm sending you a few pics taken in our wedding: www.weddingphotos4u.net/Photos/

www.fakeweddingphoto.net/

“... hover your mouse over the link. If you see that the link is not going to the place that it's from, then it's likely an email trying to steal something.”

IN THE BEGINNING IT WAS RELATIVELY HARMLESS:
PUSHING PRODUCTS TO THE MASSES



2 / 3^{rds}



of global emails
are considered spam²

12%

of email delivered to business inboxes in
2014 were spam³

SPAM - An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information. Email messages are not considered spam if a user has signed up to receive them.

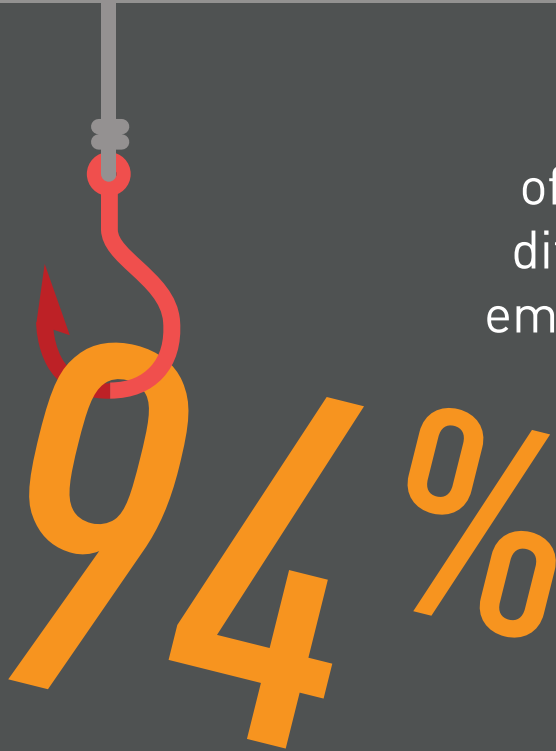
When most people hear the word “spam,” they tend to think of the obvious mass emails: ads for male enhancement pills or links to illegal online gambling. Spammers sent out millions of unsolicited emails trying to sell people things. Sometimes these were real products and sometimes they were intended to get people to buy bogus products or input their credit card information on a fake website. For some marketers, this proved to be extremely successful, and for cyber criminals, it proved an easy way to make some quick money.

But as this method became more popular, the technology industry took notice. Spam filters, especially those designed for professional use, became more advanced and got more adept at blocking these messages, thus preventing them from ever reaching a user’s inbox.

So cyber criminals evolved their techniques. They developed malicious email that was much more sophisticated, much harder to spot, and much harder for technology to detect and filter out.

In this new world, it wasn’t just about getting information or products to the masses; spam had evolved into something malicious—stealing your data, passwords and personal information.

PHISHING: HOW CRIMINALS MADE YOU THEIR PRODUCT



94%

of people couldn't tell the difference between a real email and a phishing email 100% of the time.


—McAfee: Phishing Deceives the Masses: Lessons Learned from a Global Assessment



Nearly 1 in 5

users will click on a link within a phishing email.

— 2014 Verizon investigation report



From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530



Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security. If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails, and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

[Update Your Account](#)

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.

Thank You
Outlook Warning! Member Service

Example of the Outlook.com phishing email.

Image source: <http://theworkingmouse.com/beware-of-outlook-phishing-scam/>

Just this January, nearly 400 million Outlook.com users were sent an email like the one above.

If you had clicked to update your account, you would have been taken to a pretty convincing Outlook.com website and asked to enter your login credentials.

Guess what? You've been phished! You've just given your email login to cybercriminals. Now they have access to all your email, your calendar and your contacts list. Think of all the confidential information you've just exposed.

This is "phishing" – the next evolution of spam. Phishers leveraged the email-to-the-masses approach of spam, and then evolved the threat by getting their victims to visit a malicious website or open a malware-laden attachment. All to capture your sensitive information: private documents, passwords, social security numbers, your email contacts, credit card numbers... the list is endless.

And many times, you won't even know you've been phished, until it's too late.

SOCIAL ENGINEERING – The act of manipulating people into performing actions or divulging confidential information. It relies on human interactions, such as trying to gain the confidence of someone through trickery or deception for the purpose of information gathering, fraud, or computer system access. This can take many forms, both online and offline.

PHISHING

A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people’s personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information.

SPOOFING

when a cyber-criminal masquerades as someone else (person or company) to gain an advantage or trick you into believing they are a trusted entity.

Spoofing can take many forms on the Internet, like faking the email address of another user. A spoofed website is one that mimics a real company’s site—mainly financial services sites—to steal private information (passwords, account numbers) from people tricked into visiting it.

Phishers are clever. They know users won’t fall for obvious methods. So they evolved their tactics to “spoof” trusted brands that make you more likely to click.

You may think your anti-malware software is powerful enough to identify all these emails before they hit your inbox, but phishers have evolved ways to get around many of these filters. User awareness is one of the best ways to prevent phishing links from getting clicked.

Phishing, like spam, is a numbers game: criminals send out millions of phony shipment delivery notices or banking alerts with the hopes that a few people will fall for it. And unfortunately, many people do.

Last fall, many employees at a small- and medium-sized business (“SMB”) in the UK received an email that included two free tickets to a popular production of Peter Pan happening in London.⁴ The email seemed innocent enough, but one click on the attachment containing “the tickets” infected the recipient’s computer with malware that captured corporate banking credentials.

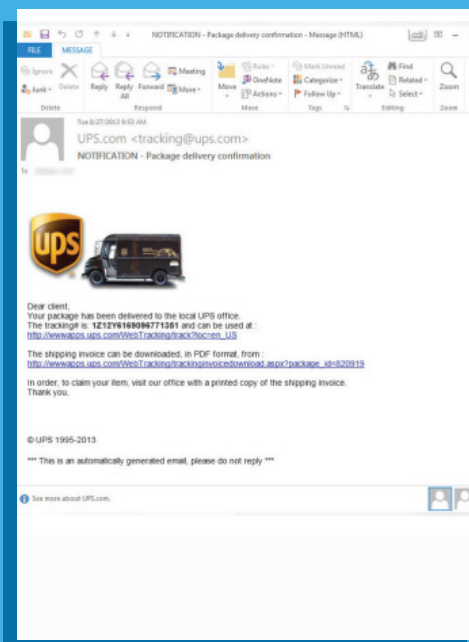
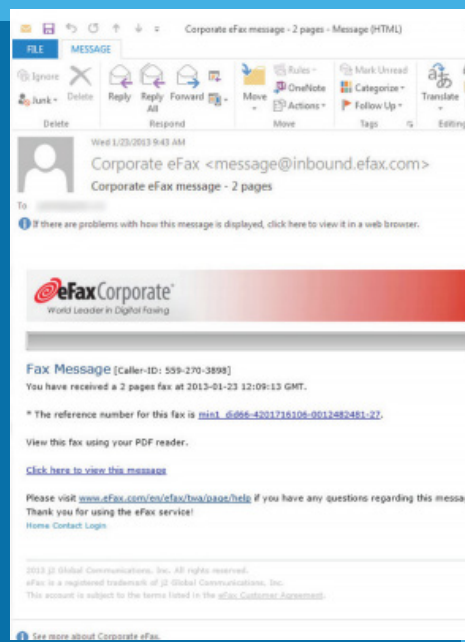
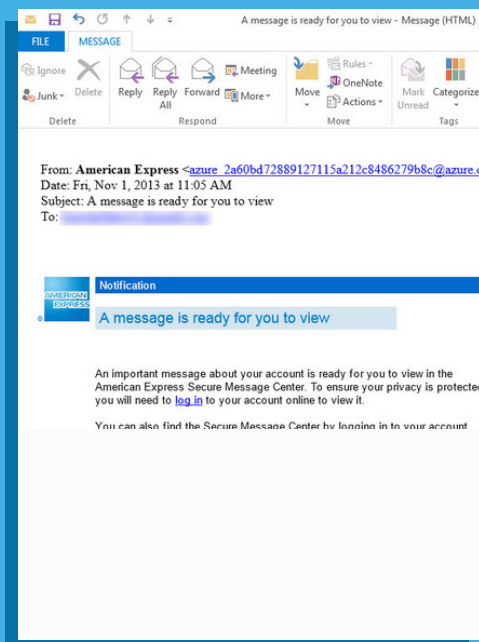
The phishers were smart. They included a link to a spoofed website matching the real theater’s site for the Peter Pan show. They referenced a real performance time and date for the fake tickets.

They knew exactly what they wanted. Their malware was set up to specifically target commercial banking logins as opposed to consumer accounts. And unfortunately, they knew that SMBs make easy targets because, in many cases, they don’t have much in the way of security mechanisms prevent phishing emails from reaching user inboxes.

But the Peter Pan attack is still an example of a mass scale phishing expedition—one based on chance.

As people have started to become more aware of phishing, attackers have needed to evolve their techniques again. Now, in order to get past all the filters and trick a smarter audience, they have set their sights on a more dangerous methodology – targeting. By combining malicious phishing tactics with “social engineering” and targeting techniques, cybercriminals have evolved phishing into a new, more vicious scam: spear phishing.

CAN YOU SPOT THE PHISHING EMAIL?



They're all malicious phishing emails that were spotted in the wild by Intel Security's team.



- Source: McAfee Phishing Quiz

SPEAR PHISHING: WHEN CRIMINALS HAVE A TARGET IN MIND

95%

OF ALL ATTACKS
on the enterprise network are the result of
successful spear phishing.

– Allen Paller, Director of Research, SANS Institute

SPEAR PHISHING - While phishing uses mass email, spear phishing targets a very small number of recipients. The email sender information may be spoofed so the email appears to originate from a trusted source. Messages typically request username and password details, provide a link to a website where visitors can enter personal information, or have an attachment containing a virus, Trojan, or spyware.

In April, 2011, employees in charge of email operations at Epsilon received an email purporting to be from a long lost friend.⁵ It seemed innocent – a friendly email announcing a recent wedding and including a link to view some photos:

Hey Neil, it's Michelle here, it has been a long time huh ? how're you doing ? how's your work with Return Path ? Is everything ok at Epsilon ? Hey, can you believe it! I got married to Brian ! Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give me your current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well, here I'm sending you a few pics taken in our wedding: www.weddingphotos4u.net/Photos/Michelle/

Let's keep in touch then.

Love,
Michelle & Brian

Reports don't say how many Epsilon employees received the email or how many clicked on the link, but at least one person did. And it only takes one to infect an entire organization.

Epsilon is a marketing services firm offering e-mail marketing and database management for many high-level clients including Air New Zealand and McDonalds. The link in the email contained three pieces of malware that infected the user's computer, exposing the email marketing lists of many of their clients.

Epsilon was one of over 50 marketing services firms to be compromised by this scam, providing cyber criminals with over a billion email addresses...email addresses of everyday consumers who'd agreed to receive marketing emails from the likes of Krogers, Walgreens, Ritz Carlton, Target, JPMorgan Chase, Verizon, Citi, ScottTrade and many more.⁶

What happened to the staff at Epsilon was more targeted than regular phishing emails. The phishers chose specific people because of their role within the company. The emails those employees received mentioned their employer and played on the likelihood that people enjoy looking at photos. They were spear-phished.

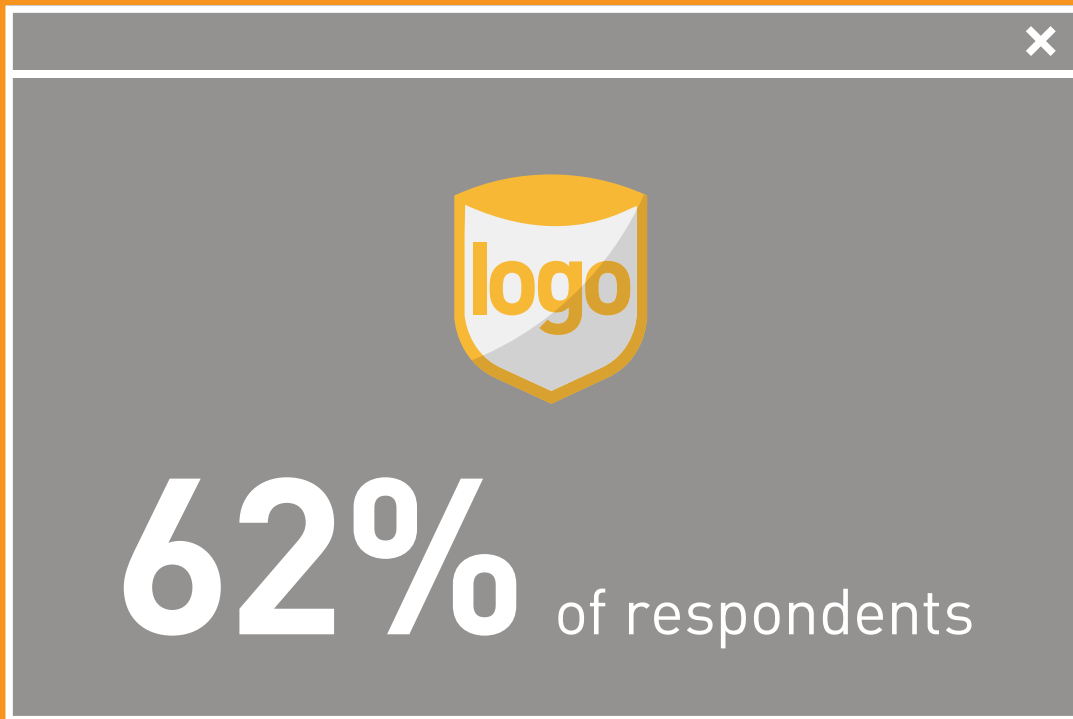
Spear phishing is highly targeted and much harder to recognize. This type of phishing is directed at a specific individual or group within an organization, and malware-laden messages are often personalized with information that leads recipients to believe they came from a legitimate source. Phishers are now using social engineering to fool their victims.

Social engineering is not a new concept. For years con artists and criminals have manipulated unsuspecting victims for their own gain. They're successful because by and large people are naturally trusting. And because so much of our lives are now online, it's much easier for criminals to engineer scams that people will believe.

To successfully manipulate a user into believing a spear phishing email is legitimate, cyber criminals often gather publicly available information about their victim. They learn about interests, hobbies, friends, colleagues and more – all to get their victim to lower their guard. They study posts on Twitter, for example, to mirror the writing style of the person they're pretending to be or include personal details that many people wouldn't think cyber criminals would know.

With spear phishing, the concern is that employees might be fooled by an email that looks like it came from an employee, from HR or from the employee's manager. And once a phisher has gotten that employee to click that link or open that file, they could have access to whatever apps or systems that the employee can access to do their job: HR systems, sales and customer information, confidential files... the potential threat is huge.

Unfortunately, cyber criminals evolved spear phishing techniques to bring them larger payoffs. And with that evolution the threat to your business became much, much worse.



in the global phishing study trusted an email that used a “spoofed” sender email address that appeared to be sent by UPS.

—Phishing Deceives the Masses:
Lessons Learned from a Global Assessment

“While people still look for identifiers such as senders name or address, subject line or content of the email, people tend to comply when a request comes from a figure of authority.”

- Hacking The Human Operating System:
The role of social engineering within cybersecurity

WHALING: WHEN SPEAR PHISHING HARPOONS THE BIGGEST FISH

FINANCIALS



96% of executives worldwide failed to tell the difference between a real email and a phishing email 100% of the time.

WHALING – A type of scam in which phishers find the name and email address of a company’s top executive or team of executives (information often freely available on the web), and craft an email specific to those people and their role at the company. The email attempts to lure the executives into clicking on a link that will take them to a website where malware is downloaded onto their machines to copy keystrokes or ferret out sensitive information or corporate secrets.

Whaling escalates the tactic of spear phishing by targeting senior executives and other leaders in key positions of influence. Whaling communications often appear to be spoofing legitimate entities that senior managers interact with—fellow executives at the company, senior leadership at partner organizations, high ranking customers, etc. These emails often prey on managers’ fears in order to provoke action.

It starts with research: attackers go to the company website and gather information on a business’s executives – names, titles, job descriptions, partner relationship, office locations and recent news. Then they scour social sites like LinkedIn and Facebook looking for details about that person so they can create a convincing spoof. It all comes down to creating a scenario that’s realistic enough to get their target to buy in.

Let’s take a look back at the Scoular Co. attack (page 5). The attacker knew the company was looking to make an acquisition in China. They knew that the CEO was travelling, and they knew the name of Scoular’s accounting firm. It was the combination of these three things that enabled the attackers to successfully fool the controller. Had they not done their research, they might not have been so successful.

In another recent case, an attacker researched the background of a systems administrator, then sent him an email about a reduced premium health care plan for families of four or more.⁷ This appealed to the administrator, who had five children, and enticed him to open the attached form. The form had embedded malware that compromised the target’s computer and gave the attacker a foothold into his corporate network. “It also allowed the attacker to impersonate the administrator and garner sensitive information about the company’s operations,” says Rohyt Belani, CEO of Intrepidus Group, a security consulting and training firm.

The moral of the story? Whaling might be the biggest threat because it targets the people who have increased access and authority, but often don’t have the time or patience to stay on top of current phishing trends. You need to assume they aren’t educated on this topic and maintain ongoing training – and not just for the executives themselves, but also their assistants and direct reports.



INTERMEDIA The Business Cloud™

Interview with Jonathan Levine

CTO, Intermedia

EMAIL SECURITY AND SPAM SEEM TO HAVE ALWAYS BEEN A CONCERN FOR BUSINESSES. WHY DO YOU THINK THERE IS A RENEWED EMPHASIS NOW?

Up until the last few years, spam has been annoying, but it hasn't really been dangerous. Now it's becoming increasingly dangerous. Hacking and malware have gradually moved from the domain of hobbyists to the domain of state actors and organized crime. So it's becoming more common and more malicious.

DO YOU THINK BUSINESSES ARE AWARE OF HOW SOPHISTICATED THESE ATTACKS HAVE BECOME?

I don't think they are, because there is a rational underestimation of the risk. It is embarrassing for an executive to admit that their controller wired \$10,000 to a bank account in Asia, so most businesses don't report these attacks and it gets under-reported. If it isn't making headlines, the likelihood of people learning about it on their own is low. This is why so many businesses don't take action and why they are at risk.

WHAT'S YOUR THEORY ON WHY THEY WAIT UNTIL SOMETHING HAPPENS TO TAKE ACTION?

I think it's human nature. We are all optimists. We don't want to believe these types of bad things can happen to us. Why do people let their auto insurance lapse or why are they underinsured? It's because bad stuff happens, but it doesn't happen to me. And most of the email you get is not malware, right? So being optimistic is not irrational. However, even though the chance that any one email exposes you to malware is small, once you get that email and click on it, you are infected. This is why the technology is so important; it's good protection—just in case.

HAVE YOU HEARD ANY HORROR STORIES OVER YOUR TENURE ABOUT COMPANIES THAT HAVE HAD PHISHING ATTACKS?

You know, I heard two horror stories just this month and they were almost exactly the same. I heard them both from people who were on boards of directors at companies where the financial controller got an email that appeared to be from the CEO instructing them to wire a large, but not alarming, amount of money to a bank account somewhere. In one case, they thought twice about it, contacted the CEO, and didn't send the money. In the other case, the controller did initiate the transfer but managed to persuade the bank to pull the money back.

ARE YOU CONCERNED AS AN EXECUTIVE ABOUT THE EMERGING TREND OF WHALING?

I am. C-suite executives suffer from the same cognitive deficits as everyone else. And even if they have higher awareness, there is that optimism that it won't happen to them. But due to their access to large amounts of intellectual property and proprietary company information, it is extremely important they do everything they can to protect not only themselves but their company.

HOW CAN BUSINESSES STAY ON TOP OF SECURITY TRENDS?

Ideally the company would have a C-level security officer, but that may only be applicable to larger companies. For smaller companies, maybe legal advisors could help keep them informed. Realistically, staying informed is practically a full time job so outsourcing your security to experts is often a great way to go for any size company.

We hear a lot of security concerns about the cloud. People seem to think that it will make your data less secure. But in reality, if the provider is taking security seriously, the cloud solution is actually more secure. Cloud providers have the means to invest much more than any single customer could. So businesses can benefit from the fact that the cloud provider has a large number of customers that they can amortize the security costs across. At Intermedia, we have a full time privacy and security team who are constantly watching the trends so they can bring any concerns to my attention and our CEO's attention immediately. This helps us stay proactive and responsive—and McAfee, as part of Intel, has a vast security army.

WHAT ARE THE BENEFITS OF MANAGING SECURITY UNDER ONE PROVIDER?

The most vulnerable point of security is when data is being moved. So if you keep the data in one place you reduce the number of vulnerability points. But of course, if your single provider does suffer some kind of a security breach, that could be a big problem. It is so important you choose a provider that invests heavily in security. There has been a lot of talk lately about encryption of data at rest. This is when data is stored at a cloud provider or a service provider, but it's encrypted in a way that even the service provider can't get access to it. This offers the highest levels of security in multi-tenant environments. Businesses should do their due diligence when choosing a cloud provider to ensure they offer advanced security measures, like encryption at rest, to help mitigate the risks.

HOW DO YOU THINK INTERMEDIA IS WORKING TO MITIGATE AGAINST EMAIL SECURITY RELATED ISSUES?

From a technology perspective, we have a separation of networks and systems in place to act as a second layer of defense. For example, even if a system administrator's PC is compromised, it's difficult for an attacker to actually use that compromised PC to get access to a sensitive system. We also have good detection systems in place so that if something is compromised we know about it quickly, and we can do something about it before information is lost.

As a company, we have a dedicated security and privacy team who do a lot in regards to employee education. They continually monitor the newest threats and they create simulated attacks on our employees. We understand the biggest area of vulnerability, due to spear phishing, is employees who have access to data. And our system administrators have significant privileges into our systems, so we make sure they are educated frequently on trends and constantly on alert. It's quite helpful for us and assures our customers of how seriously we take security.

ANY FINAL WORDS FOR BUSINESSES THAT MIGHT BE READING THIS?

My best advice is to stay smart about security. Take precautionary steps now to prevent attacks later.

HOW TO PROTECT YOURSELF

There isn't one solution for email security. Phishing comes in many varieties, and that makes it impossible to implement a "one size fits all" strategy to stop it. The best defense includes a combination of tactics – both technological and psychological.

We suggest a three step process:



1.

Educate your users and executives

Employee education is your best defense against many kinds of hacking attacks. If users don't fall for the phishing scam, attacks usually don't happen. We recommend leading your employees and executives through interactive training sessions. The concept is to simulate real security attacks like spear phishing to lure employees within a safe environment. So if they give away passwords or click links they can safely learn from their experience.

Additionally, it's also good to give your employees something they can keep at their desks to refer to later. We've developed a list of best practices that can be printed to remind users of the dangers of phishing to help them avoid falling for the scams.

2.

Deploy comprehensive protection and protect your "attack surface"

Technology offers multiple layers of protection to help fend off spam, viruses and spear phishing attacks by preventing some malicious emails from reaching user inboxes. And while it can't replace user education it may help reduce the impact of an attack if users do fall victim.

Using anti-malware filters in combination with real-time URL scanning gives companies a second layer of defense. Protecting your "attack surface" by regularly auditing your distribution lists and externally accessible email addresses can close up some of the avenues that phishers use to send email through to your employees' inboxes.

3.

Plan for the worst case scenario

Once you have been targeted by an attacker you have to rely on technology and employee awareness to thwart the attack. Smart companies understand these two safeguards aren't always effective and harden their infrastructure to help minimize the impact of a potential attack. This means looking beyond email to how sensitive data is stored and accessed. The goal is to keep your data accessible to the right people while keeping it out of the hands of the wrong ones.

Solutions like single sign-on, email archiving, secure file sync and share and data loss prevention all work to give you an additional layer of security. And it is always recommended to have a dedicated security expert on staff but if that isn't possible, make sure your business is monitored by outsourcing to a trusted hosted provider.

LET'S NOW DIG DEEPER INTO THESE TOPICS.

EDUCATE YOUR USERS AND EXECUTIVES

1
STEP



“Forewarned is forearmed” as they say. Building awareness of email scams and the motivations behind them is one of the most important things you can do to reduce your company’s vulnerability to an attack.

But you can’t just train once; you need to continually educate your employees.

All the preventative technology in the world won’t stop every phishing attack if business users fall for the phishers’ tricks.

The best way to educate your employees, including your executives, is by leading them through active learning exercises. A prime example of this is Facebook’s annual Hacktober initiative.

Facebook times Hacktober to coincide with the National Cyber Security Alliance’s (NCSA) annual National Cyber Security Awareness Month for added relevance. They stage simulations of real-world security attacks like phishing emails and thumb drive drops. The concept is create a safe environment where employees can make mistakes and learn. So if an employee clicks on a link or gives up a password, they can learn in a safe way. You can find more details about Facebook’s efforts in this article from AdWeek: www.adweek.com/socialtimes/how-to-hacktober/439382

This event has been very successful at Facebook and is recommended by Ryan Barrett, Intermedia’s VP of Security and Privacy, as one of the best methods to teach employees. “An employee’s personal experience, whether they fell for the staged phishing email or saw through the ruse, makes them the perfect security evangelist to their fellow employees and partners.”

Of course, Facebook is a large company with a dedicated security team that can easily plan and run a complex educational initiative like Hacktober. What about a smaller company with one person in charge of security? Or no dedicated security staff? Not to worry. Even if you don’t have someone inside the company who can run these types of exercises; there are companies out there, like PhishMe, which can help.

It’s also good to give your employees something they can keep at their desks and refer to later. We’ve developed this list of best practices that can remind your users of the dangers of phishing and help them recognize and avoid such scams.

BEST PRACTICES TO AVOID BEING PHISHED

Keep your security software up to date. Don't avoid downloading important updates, hackers exploit vulnerabilities found in older software, so it's important to keep the apps on your devices current.

Be aware of email requests with high urgency and quick action. Phishers often prey on employee trust and will spoof executives to get you to comply with high urgency actions like wiring large amounts of money ASAP. If you are ever in doubt, double check the request with the sender either by phone or by composing a new email—never reply to the email itself.

Never give personal or financial information over email. Trusted parties will never ask you for personal information through email. Try to make it a known company policy not to collect employee information (ex. social security numbers, account numbers, credit card numbers, etc.) internally via attachments or divulge information to partners via emails.

Don't click on links from messages that contain misspellings. If an email from a well-known company is formatted badly, has obvious misspellings or is unrelated to the product or company, this is a red flag.

If an offer seems too good to be true, it probably is. Big bonuses, large payments or gifts (ex. win a free iPad) for services are ways attackers try to get inside your head. If the promise is "too good to be true", do some research into the individual or company before taking action.

Think about whether you initiated the action. Phishers will try to spoof well-known companies to have you reset your password, update your account or track a shipment. Always be suspicious of unsolicited email, if you didn't prompt a password reset — don't click the link.

Be careful about what you post publicly to social networking sites.

If your social networking profile is public, avoid sharing birthdays, kids' names, or detailed business information. Attackers will use this information to learn more about you for spoofing purposes or to get clues about what your passwords might be.

Stay educated on phishing techniques. Spammers are constantly evolving their techniques. Staying up-to-date on the latest types of techniques and threats is the best way to protect yourself. Commonly, these attacks look like urgent emails coming from a boss or colleague, and attachments tend to look like a voicemail, fax or shipment tracking slip.

Act quickly If you accidentally click on a link or think that you have been phished, the quicker you take action the better. Talk to your IT department, put a stop on a wire transfer or alert other people in the organization — immediately.

You can print these out here bit.ly/1PU5R1L and distribute them to your users so they always have a quick reference.

INSTALL COMPREHENSIVE PROTECTION AND PROTECT YOUR “ATTACK SURFACE”

2

STEP



Technology offers multiple layers of protection to help you fend off not just spam and viruses but also sophisticated spear phishing attacks. And while it can't replace user education, it can reduce the impact of an attack if users do fall victim.

Implement anti-malware filters and real-time URL scanning

Anti-malware filters can prevent some malicious emails from reaching user inboxes in the first place. But you can't stop there. You need real-time URL scanning, too. The URL scanning component runs a secondary scan to check for changes in URL intent that occur between the time the message is first delivered to the user's inbox — regardless of how harmless it may appear — and the time the user clicks on it.

Move your email to the cloud with a trusted hosted provider

A benefit of moving to the cloud is it allows companies the freedom to focus on what they do best, while the experts manage their email security. For many companies, IT budgets are tight and having a dedicated security expert on staff can be cost-prohibitive.

The beauty of moving to a hosted model comes from the fact that a hosted Exchange provider's reputation rests in part on its ability to offer a more secure environment than many businesses could on their own. A good hosted Exchange provider will invest heavily in the security of its cloud, at a rate that most individual businesses can't replicate with an on-premises email setup. This includes partnering with top-rated security application providers, implementing stringent datacenter security measures, and continually educating its own workforce on phishing tactics.

Additionally, a trusted hosted provider can help you stay on top of security trends. They should alert you to the latest phishing scams, offer tips and tricks to avoid falling victim and employ an army of experts who can assist if you do get attacked. It's always best to have your own dedicated security personnel, but if that isn't possible, you should consider outsourcing to a trusted provider.

Of course, you need to do your homework when shopping around for cloud-based email. Don't just go with any provider because they offer the best deal. You'll find that many of the best hosted Exchange providers will spotlight their security capabilities by having them measured against a well-established auditing standard, such as SSAE 16 Type II, PCI, or especially SOC 2 Type II.

ATTACK SURFACE – the aggregate of all vulnerabilities and controls across all systems and networks. It is the collection of targets exposed to an attacker. ⁸

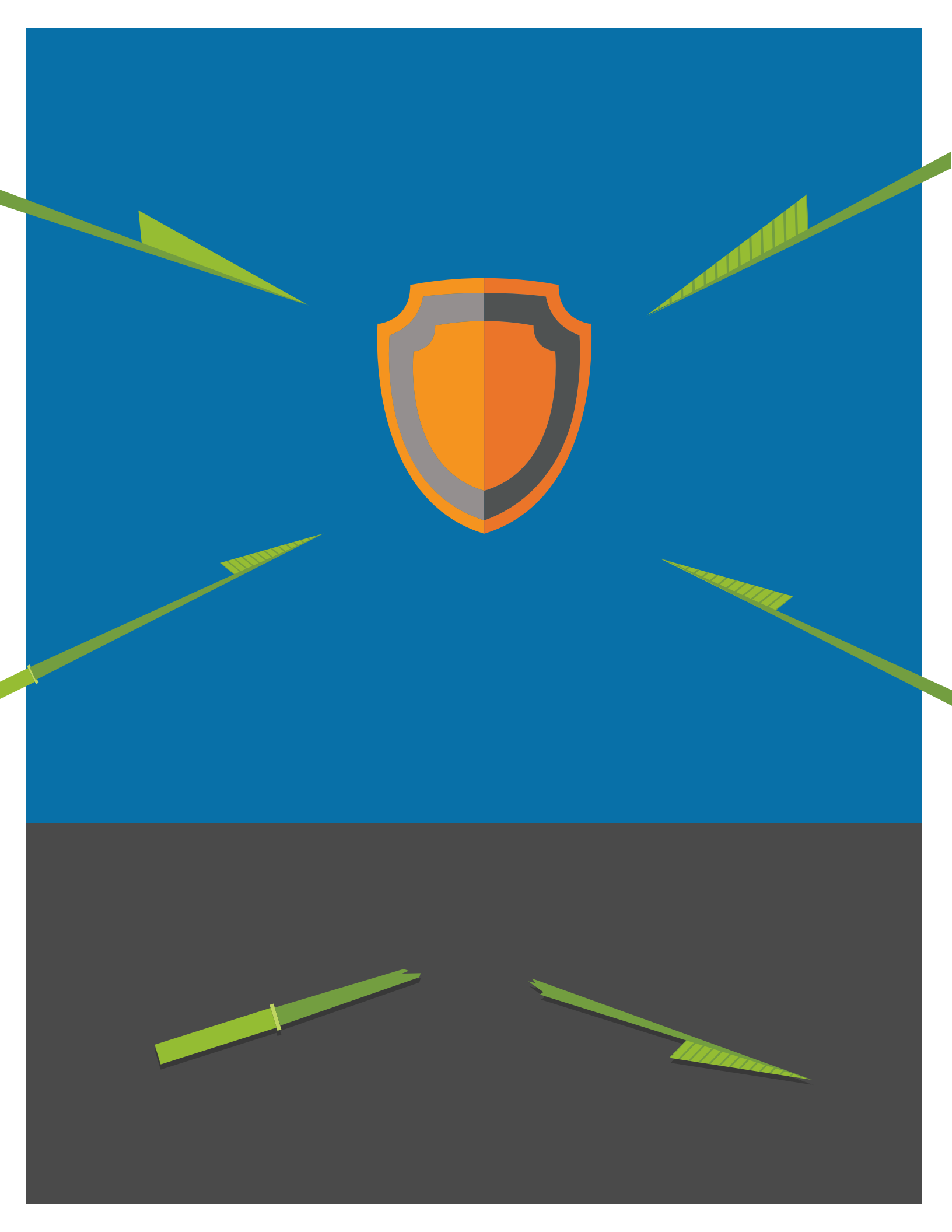
Protect your ‘attack surface’.

Spear phishers looking for passwords can be your biggest enemies. They are sending targeted emails, and not mass quantities of spam. These emails can get through technical barriers because the IP address that they are using looks safe to anti-spam filters. There are no viruses or malware behind the URLs, just password capture forms. So the best way to really protect your company from these types of attacks is user education.

Attackers know that if they want to phish your company, they have to get their emails through your outer perimeter – your attack surface – and into your users’ inboxes. One of the most common ways they get through is by using distribution lists (DLs) and email addresses that are reachable from outside your company.

We recommend that businesses monitor email and distribution list rules to close gaps that could be exploited for phishing. It stands to reason that sales@yourcompany.com would need to be an externally accessible address, but that’s not true of addresses like facilities@yourcompany.com or for a DL that’s been created for an internal project.

But this isn’t a “one and done” effort. You need to go in frequently and clean up what you have. We also recommend that you put a process in place so that any new lists or email addresses that require outside access need to be vetted and approved by IT.



PREPARE FOR THE WORST

3

STEP



Once someone has targeted you, you need to protect yourself by hardening your infrastructure. This means looking beyond email to how your sensitive data is stored and accessed. You need to implement tools that can protect your IP while still enabling your employees to effectively do their jobs. The goal is to keep your data accessible to the right people while keeping it out of the hands of the wrong ones.

Use a single sign-on solution to protect passwords

If someone gets your email password, they have access to all your messages. If you have stored any passwords in an email folder or in an attachment, the attacker will now have access to them, too. The best way to solve this problem and to keep your passwords secure is to use a single sign-on solution (SSO) with 2 Factor Authentication (2FA). The SSO application will remember all of your passwords for you, including CRM apps, financial apps, file sync and share, and more. You just need to know one username and password to log in to your SSO portal. 2FA adds an extra layer of protection by also requiring you to enter a login code that's delivered to your mobile device. So even if an attacker were to obtain your SSO password, they would still need your phone to access your SSO portal.

Protect sensitive data with secure file sync and share

If everyone is using personal file sync and share to store company IP, the IT manager can't protect that data. Phishers could gain access to the data, or even worse, the data could be encrypted and held for ransom. Businesses should consider company-approved, secure file sync and share solution. That way, the IT manager has access to all company data, which is stored in a central location, and can therefore change passwords and help prevent an attacker from locking the company out.

Additionally, we recommend that businesses consider not using attachments internally in order to lower the risk of accidentally opening malware. With a secure file share application, important documents are shared via web links that are encrypted in transit and can be protected with passwords.

Save all your emails securely with email archiving

Employees tend to keep a lot of data in their inboxes, using them like a data repository. And for many businesses, regulations require that emails be saved for certain periods of time. However, this is dangerous because it gives phishers access to years of historical data, which they could use against you or destroy. With email archiving, you can delete emails out of your inbox knowing they are saved securely in your archive, outside of Exchange. Should a cyber-criminal destroy any data in a user's inbox, the eDiscovery capabilities of your archiving tool will make restoring lost messages fast and easy.

Prevent spoofing with outbound email monitoring

It used to be that cyber criminals wanted access to your systems to create zombie farms to spam the masses. While that sometimes still happens, most attackers are taking it to the next level. They want to spoof your company to spear phish YOUR customers and partners. You need to take steps to not only protect your inbound communications but also to monitor your outbound communications.

An outbound monitoring application will scan emails that leave your company for malicious URLs and attachments. This scanning tool can also prevent sensitive information like customer contacts or corporate IP from leaving via email – either in the message body or in an attachment. With outbound monitoring installed, you can more easily quarantine your email system if a malware infection does happen so that it doesn't become a vector that the phisher can use to cause more destruction.

Look for a good hosted email provider that will offer you outbound monitoring in combination with email continuity. This way your employees can continue to send and receive email while the infected mailboxes are isolated and the damage is repaired.



AGIO

Interview with Bart McDonough CEO, Agio

WHO IS AGIO AND WHAT SERVICES DO YOU RESELL?

Agio is a managed IT and cybersecurity services firm, focused specifically on the alternative investment space. We are an Intermedia user and reseller as well as Intel Security, among other partners. Our full suite of services includes Remote Monitoring & Management of client infrastructure, End User Support, Hosted Solutions such as Managed Backup, Private Cloud Offerings, and Managed Disaster Recovery. We also have a deep cybersecurity practice, providing clients with Managed Security, Consulting, Policy Writing & Development, and Assessment work, such as Risk Assessments, Penetration Testing, Vulnerability Assessments, etc.

SINCE YOU FOCUS ON CYBER SECURITY, WHAT DO YOU DO TO HELP YOUR CLIENTS?

We spend a significant amount of time educating. People don't know what they don't know. We just conducted an email phishing campaign for a client, who wanted a "Capture-the-flag" exercise. Our security team deployed a phishing test, determined their vulnerabilities and then were able to penetrate their network. We accessed their servers, viewed their browser history and logged in as an internal user to view proprietary documents; all of which we then presented to the client as the results.

Our objective here is always to raise awareness within the organization of the dangers and impact of phishing, if executed successfully. Sometimes we have to go to these lengths to really open management's eyes to the dangers and risks of an attack. It's highly effective.

WHAT BEST PRACTICES DO YOU RECOMMEND YOUR BUSINESS CLIENTS EMPLOY TO HELP WITH USER EDUCATION?

There's a few different things; obvious spelling errors, emails that prey on your emotions or create urgency, modified URLs and nonspecific to/from fields. Almost as important, we teach our clients to slow down and think about the email; ask yourself things like, do you normally receive an email from this organization? Is this something that's out of the ordinary? If the email asks you to do something, rather than clicking the link in the email, we recommend logging into your account to execute what the email is requesting. That way you can verify the sender's legitimacy before clicking on something potentially malicious.

Those are the biggies. We also use McAfee ClickProtect, and I love the extra layer of protection it provides behind the scenes. When you're having a busy day and are quickly running through emails, it's so much easier to fall prey to phishing. I really sleep easier knowing I have ClickProtect to add that second layer of protection; so much so that I wish I had it on my personal accounts as well.

HAVE YOU FOUND THAT THERE ARE PARTICULAR INDUSTRIES THAT ARE MORE OR LESS SUSCEPTIBLE TO THESE TYPES OF ATTACKS?

It's really an opportunistic threat profile. If you think about it from the bad actors point of view, they're casting as wide a net as possible, dropping phishing emails left and right to see who bites. I think as they become more sophisticated, they'll start targeting firms with more access to funds. To that end, we certainly think the financial services community will be one of the first to experience more direct, targeted attacks. However overall, we still feel it's a pretty opportunistic game; there are a lot of phish in the sea – so to speak.

HOW DO YOU AND YOUR TEAM STAY CURRENT ON SOME OF THE LATEST SECURITY TRENDS?

Great question. Among other boards and forums, we're a member of the ISAC organization, specific to the financial services community, which shares data among various organizations, from service providers to the actual end businesses, who are impacted. We're also constantly participating in roundtables and other security forums to understand the evolution of the threat landscape.

Staying educated on trends will always be a challenge for any firm, but staying on top of it is really the only way you can intelligently defend your environment.

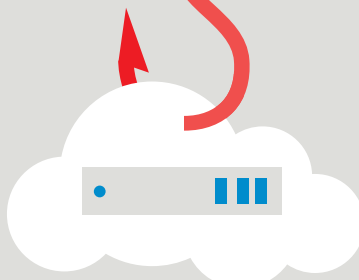
HOW CONCERNED DO YOU THINK BUSINESSES SHOULD BE ABOUT PHISHING?

Businesses should absolutely be concerned and aware of this issue. Every C-suite and every board member at a firm should be able to answer the question, "What are you doing around your cyber security policy? Specifically, what are you doing to protect against phishing, spear phishing, etc.?" They might not know the intricacies of the application and technology or when the training actually takes place, but they should understand the key tenets of it, like "We conduct training twice a year." They should have that on the tip of their tongue, but I think we're still a long way from that.

CONCLUSION



Money



Intellectual
Property



Reputation

Every day, more and more stories of phishing attacks appear in the news. Companies large and small are losing money and confidential data and exposing customers and partners to subsequent attacks.

If you haven't already taken steps to protect your business, now is the time. Technology plays an important part in preventing phishing attacks, but when coupled with thoroughly and continually educating your employees and your executives you can stop cyber criminals in their tracks.

All it takes is one person to click a link or open an attachment for your company to be infected and your company data and reputation to be at risk. Don't wait until an attack happens to realize the seriousness of the threat. Take protective action today!

Intermedia Hosted Exchange

<http://www.intermedia.net/products/exchange-hosting>

With Intermedia Hosted Exchange, company email is managed in the cloud as a service, with no fees upfront. Businesses get all the functionality of Exchange without all of the overhead. We perform all installation, maintenance, upgrade and support activities for a predictable monthly fee. We offer a 99.999% uptime guarantee, 24/7 support, with typical hold times of less than 60 seconds, and free migration performed by our experts. We regularly obtain a SOC 2 Type II audit report from an independent auditor to validate that, in their opinion, our security related controls and processes were effective during the evaluation period. We are audited company-wide against all five trust service principles: security, availability, processing integrity, confidentiality and privacy.

Intermedia AppID® for single sign-on

<http://www.intermedia.net/products/appid>

Intermedia AppID enables users to access their web apps with just one password, eliminating the temptation for them to take password shortcuts that can introduce security holes. Two-factor authentication protects access to sensitive applications for all employees or just a subset of them. IT Admins can also configure the session timeout period to control how often users have to re-enter their Intermedia AppID login credentials. What if a user's device is lost or stolen? What if the user leaves the company? With Intermedia AppID, IT Admins can revoke a user's access to their portal in one click. This provides excellent protection against unauthorized access to company data and services.

Intermedia SecuriSync® for secure file sync and share

<http://www.intermedia.net/products/SecuriSync>

Intermedia designed SecuriSync to ensure high security of data, to reduce the chances of data being accidentally deleted, and to provide easy ways to backup, restore and recover data should it be lost. Web links allow users to share individual files with users both inside and outside of the company, without giving users permission to view or edit other documents in the same folder. For additional security, web links can be protected with passwords. IT Admins can restore deleted files and prevent permanent deletions. And SecuriSync is one of just a few collaboration solutions to allow administrators to wipe data remotely. In case of a lost or stolen laptop, tablet, or mobile phone, or when facing a personnel issue, corporate data can be quickly removed, minimizing potential data leakage.

Intermedia Email Archiving

<http://www.intermedia.net/products/email-archiving>

Intermedia's Email Archiving helps provide preservation, protection and recovery features that meet or exceed the standards necessary to facilitate compliance—while speeding eDiscovery and helping to safeguard valuable intellectual property. We automatically capture and store every email and every attachment received by every mailbox that has activated the service. Once an email is stored, it remains searchable, accessible and secure. We keep all email messages and attachments in their original form to make eDiscovery easier. And unlike other vendors, Intermedia keeps that data online and never migrates it to offline or near-line storage systems.

McAfee Advanced Protection with ClickProtect

<http://www.intermedia.net/products/mcafee-email-protection>

This sophisticated solution leverages the highly rated McAfee gateway AntiMalware Engine in combination with scan-time and click-time URL protection known as McAfee ClickProtect. It works from any device, anywhere, to help thwart spear phishing attempts. With ClickProtect, at the time a URL in an email is clicked, it asks the question: "Is the URL still safe?" All delivered URLs are rewritten and inspected and rescanned by the anti-malware engine, using behavioral emulation to detect malicious web content without the need to rely on a signature. A safe preview allows users to view malicious websites safely and learn best practices, adding another layer of security and reducing overall risk. Messages can be safely forwarded, and, even if recipients don't have ClickProtect, the protection follows the email everywhere it goes.

McAfee Data Loss Prevention

<http://www.intermedia.net/products/mcafee-data-loss-prevention>

McAfee Email Data Loss Prevention filters outgoing email to help prevent sensitive information or undetected viruses from leaving a user's outbox. Using McAfee's web console, you can filter content using keywords and patterns to spot sensitive information and prevent viruses, worms or other malicious content from infecting recipients.

FOR MORE INFORMATION, CALL US AT 877-237-2183.

ABOUT INTERMEDIA

Intermedia is a one-stop shop for cloud business applications. Our Office in the Cloud™ suite integrates the essential IT services that companies need to do business, including email, voice, file syncing and sharing, conferencing, instant messaging, identity and access management, mobility, security and archiving. We bring these key services together under one login and one password, with one bill and one source of support to give you the freedom to focus on business instead of on your IT services. We provide enterprise-grade security, a 99.999% uptime SLA and 24/7 phone support with typical hold times of less than 60 seconds. www.intermedia.net

Note: Intermedia, the Intermedia logo, Office in the Cloud, SecurSync and Intermedia AppID are registered trademarks or trademarks of Intermedia.net, Inc. in the United States and/or other countries.

ABOUT INTEL SECURITY

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique McAfee Global Threat Intelligence, Intel Security is intensively focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

No computer system can be absolutely secure.

Note: Intel, the Intel logo, McAfee and the McAfee logo are registered trademarks of Intel Corporation in the United States and other countries. Other names and brands may be claimed as the property of others.

1. Omaha's Scoular Co. Loses \$17 Million After Spearphishing Attack, CSO Online

<http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoluar-co-loses-17-million-after-spearphishing-attack.html>

2. McAfee Labs Threats Report, February 2015

3. Radicati Email Statistics Report, 2014 - 2018

4. Attack Steals Online Banking Credentials from SMB's, Information Week's DarkReading.com

<http://www.darkreading.com/attacks-breaches/attack-steals-online-banking-credentials-from-smbs/d/d-id/1315615>

5. Epsilon breach used four-month-old attack, iNews.com.au

<http://www.itnews.com.au/News/253712,epsilon-breach-%20%20%20%20used-four-month-old-attack.aspx>

6. Epsilon Breach Raises Specter of Spear Phishing, KrebsSecurity.com

<http://krebsonsecurity.com/2011/04/epsilon-breach-raises-specter-of-spear-phishing/>

7. How to stop your executives from being harpooned, InfoWorld.com

<http://www.infoworld.com/article/2621583/phishing/how-to-stop-your-executives-from-being-harpooned.html>

8. Infosec institute; www.resources.infosecinstitute.com/attack-surface-reduction/



INTERMEDIA

The Business Cloud™

For more information:

CALL US
877.237.2138

EMAIL US
sales@intermedia.net

ON THE WEB
intermedia.net