



FOS IN THE NEWS SPECIAL EDITION: PHISHING

Phishing—the stealing of money, information, and access, through fabricated emails or other communications which falsely misrepresent the sender’s identity—has become a common problem for businesses of all sizes.

Over the past few months, FOS has seen a dramatic increase in many types of phishing attacks on corporations and their employees.

FOS clients have already been targeted, and others will be targeted in the future.

Known 2018 phishing email incidents were up 60% over 2017, when FOS issued its initial Client Alert on the issue.

That Alert, which discusses title company phishing, is located at <http://foslaw.com/news-views/client-alert-wire-transfer-fraud/>.

It is estimated cybercrimes will directly and indirectly cost businesses \$5.2 trillion over the next five years.

Phishing attacks have become so sophisticated that their targets may not know they have been victimized. This is true, even if they are generally aware that these scams exist.

Also, each type of scheme can morph into a different scheme upon its discovery.

Phishing is not a new subject for this newsletter.

For example, the fraudulent phishing of employee compensation was addressed in shareholder **Matthew O’Neill’s** article, “Gone Phishing – For Paychecks.”

That article, which appears on the front page of FOS’s Summer 2019 newsletter, can be accessed at <http://foslaw.com/about/newsletters/>.

Given cyberfraud’s prevalence and the financial losses which can occur from a successful attack, FOS is dedicating this entire issue to addressing this scheme.

Articles in this issue discuss what phishing is, tips to help prevent it, what to do if your company is attacked, and the availability of insur-

ance to defray cyberfraud losses.

FOS’s attorneys stand ready to guide you and your company through this increasingly perilous danger.

Sources:
www.forbes.com/sites/kellyphillips-erb/2018/12/04/irs-warns-on-surge-of-new-email-phishing-scams/#7fae957a4b24

<https://securityboulevard.com/2019/01/cybercrime-to-cost-5-2-trillion-over-next-5-years-high-tech-industry-most-at-risk/>

PHISHING’S UNENDING DISGUISES

When FOS first encountered cyber attacks in communications to the firm, our clients and contacts, the communications themselves barely tried to disguise their fraud.

Now, phishing is extremely sophisticated.

Fraudulent emails appear professional and genuine, supposedly coming from real company employees

under accurate company letterhead.

The fake email on page 2 is one of an unending number of ways a phishing attack may present itself.

An uneducated HR or inattentive accounts payable employee might not give a phishing communication a close examination.

If so, the employee may not

notice that the sender’s email address is different by one letter-from the real contact.

Or that the “new” payment address is in a state where the company does not operate.

Or that the “new” payment routing instructions are to an account in a different name from the real company’s existing account.

Instead of paying an actual vendor’s bill or a real employee’s payroll, the employee, complying in good faith with a supposedly accurate request, may send money to a scammer across the world.

Two examples of actual phishing attacks highlight the scams’ real dangers.

Continued on page 2



IT LOOKS REAL - BUT IS IT?

You are the head of payables. You receive this email, apparently from your Waukesha vendor, Your Vendor, Inc. Your contact's email address at that company is david@yourvendor.com. The email initially appears above-board. Closer inspection however, reveals it is a phishing attack. Small hacking changes can spell big trouble for your company.

Friday 9/27/2019 7:58 PM

From: David@_yourvendor.com → **Not vendor's email (should be david@yourvendor.com)**

Date: 2019-09-13 10:04 AM (GMT-05:00)

To: Payables Department

Subject: New Remittance Instructions

Dear Customer: → **Not vendor's name (should be Your Vendor, Inc.)**

Effective October 1, 2019, [YourVendor, Inc.](#) has new locations for your payments as listed below.

Please make this change so your payment will be timely received and applied.

Check Payment:

[YourVendor, LLC](#) → **Different company name (should be Your Vendor, Inc.)**

155 X Street

[San Diego, California 92101](#) → **Not vendor's address (should be Waukesha, WI 53186)**

Wire Transfer/ACH:

JPMorgan Chase Bank

[San Diego, California](#) → **Not vendor's address (should be Waukesha, WI)**

ABA# 12345678910

Account# 11121314

Account Name: [YourVendor, LLC](#) → **Different company name (should be Your Vendor, Inc.)**

For help with wire transfer/ACH payments, click here ([link](#)) → **Link to fraudulent service platform**


We value your business. If you have questions, call 888-750-7889.

Your Vendor, Inc.

P.O. Box 5678

[Chicago, Illinois 60610](#) → **Not vendor's address (should be Waukesha, WI 53186)**

David@_yourvendor.com → **Not vendor's email (should be david@yourvendor.com)**



Phishing's Disguises, continued from page 1

In one example, a wrongdoer, posing as an employee, emailed the employer's human resources department. The email directed that the real employee's future payroll checks be deposited in an account controlled by the wrongdoer.

The human resources department believed the request was

valid, and complied, depositing the real employee's pay into the wrongdoer's account.

By the time the real employee noticed he was not paid, the money had vanished, likely to a foreign country.

In another example, a company received a bogus email, supposedly from an existing supplier. The email gave a new address, wire and ACH

instructions for payments. Because the email, which contained the supplier's letterhead, did not look suspicious, the company complied, sending its checks to a new address.

Only after multiple checks were cashed did the company discover that the "new" instructions were a scam. The vendor had not received at

least \$75,000 in payments. The company had obtained cyber insurance which covered the scam. Because of its large deductible, however, the insurance covered only one third of the current loss.

Every company is a potential phishing victim. For tips on fraud prevention and defenses, see the remaining articles in this newsletter.

GO BACK TO BASICS TO AVOID DATA BREACHES

The best defense against phishing hacks may be old-fashioned common sense—verify, verify, and verify:

Make all employees, especially HR and accounting employees, aware of data breach schemes.

Charge appropriate employees with the duty to red-flag suspicious activity for verification.

Establish protective/verification protocols and advise vendors, customers

and financial institutions of them.

Designate at least two appropriate employees to independently confirm and document the accuracy of information/document/payment requests, before disclosing financial/confidential information or making a payment/account change, etc.

Do not comply with oral (telephone or voicemail) **change requests**.

Require a delay for verification of requests for financial/confidential information, payment, or changes to addresses, account numbers or routing instructions.

Do not trust requests via emails, texts, or other writings, even if they appear proper. Verify.

Instruct employees to not hit “reply” or click on a link in an email or text, which can lead to a wrongdoer’s fraudulent platform.

Verify requests through telephone conversations (at known numbers) or, if possible, face-to-face verifications with the person requesting a change.

Obtain appropriate insurance covering cyberfrauds and cybercrimes.

If a request looks suspicious, it probably is. Even a request that looks totally proper, however, can still be a scam.

IF THE WORST HAPPENS, ACT!

Despite the best preventative measures, at some point you or your company may be the victim of a phishing attack.

If this happens, don’t panic.

Instead, immediately take action to stem your losses, perhaps recover some of the stolen funds, and prevent further attacks.

Notify your financial institution(s). Place a block on or otherwise secure any potentially affected account until you conduct a proper investigation.

When your investigation is complete, make a claim, if appropriate, for reimbursement against the proper financial institutions.

Change email addresses, passwords, security questions/answers, wire transfer

protocols, and other existing security information.

Notify all affected vendors, employees, companies, etc. of the attack and its circumstances.

Advise them of the steps you are taking to protect against another attack.

Assure them that you are seriously addressing the issue and ask them to contact you if additional problems occur.

Notify other vendors, employees, customers, material contacts, etc. of the attack, its circumstances, and the potential for future attacks.

As with affected vendors, advise them of the steps you are taking to protect against another hack.

Notify law enforcement including, if appropriate, the FBI and IRS.

The FBI’s website addressing cyberbreaches is at <https://www.fbi.gov/investigate/cyber>

The IRS’s corresponding website is at <https://www.irs.gov/individuals/taxes-security-together>.

Investigate your computer system, including your email system, to determine the extent that cyberfraud or other intrusion(s) has/have occurred.

Notify and file a claim with your insurance carrier. If you have no insurance covering phishing losses, have your insurance agent determine whether an appropriate policy is available.

Implement your company’s cybersecurity procedures. In doing so, investigate which procedures worked well, which need practice, and which need revision.

If your company has not created a cybersecurity policy, now is the time to do so.

A cybersecurity policy can help prevent future cyber attacks.

Your IT representative, insurance agent, and FOS attorney can help you create, implement, review and revise an appropriate data breach policy.

QUESTIONS?

CALL US
414-273-3939

EMAIL
info@foslaw.com



622 N. Water Street
Suite 500
Milwaukee, WI 53202
Phone: 414-273-3939
Fax: 414-273-3947
www.foslaw.com

Fox, O'Neill & Shannon, S.C. provides a wide array of business and personal legal services in areas including corporate services, litigation, estate planning, family law, real estate law, tax planning and employment law. Services are provided to clients throughout Wisconsin and the United States. If you do not want to receive future newsletters from Fox, O'Neill & Shannon, S.C. please send an email to info@foslaw.com or call (414) 273-3939.

Address label

IN THIS ISSUE

Page 1 FOS Special Edition/
Phishing's Unending Disguises

Page 3 Avoid Phishing/If the
Worst Happens, Act!

Page 2 It Looks Real - But Is It?

Page 4 Does Your Insurance
Cover Phishing Losses?

This newsletter is for information purposes only and is not intended to be a comprehensive summary of matters covered. It does not constitute legal advice or opinions, and does not create or offer to create any attorney/client relationship. The information contained herein should not be acted upon except upon consultation with and the advice of professional counsel. Due to the rapidly changing nature of law, we make no warranty or guarantee concerning the content's accuracy or completeness.

DOES YOUR INSURANCE COVER PHISHING LOSSES?

The articles throughout this newsletter highlight the importance of obtaining appropriate insurance to cover losses from phishing and other cyberfrauds.

Indeed, there appear to be as many types of insurance policies as there are frauds.

Unfortunately, given cyber-fraud's recent and rapid development, and its ability to change from one form to another, neither the insurance industry nor the law has settled on the meaning of insurance coverage language.

In short, even if you intend- ed to and believe you have obtained adequate insurance

cyberfraud coverage, an insurer may deny coverage based on a specific policy's wording as applied to a particular wrongful act.

Some courts, for example, have considered whether losses from fraudulently manipulated emails, whose requests for the wire transfer of funds to cyber criminals were unwittingly granted, constituted covered "direct losses."

The trial courts in these cases initially ruled that these phishing scams did not result in "direct losses," and so no insurance coverage existed for the insured's damages. The appellate courts eventually ruled in the insureds' favor.

To achieve these results, however, the insureds had to spend the time and money to challenge the trial courts' rulings.

Moreover, even policies specifically "covering" computer fraud may not, depending on their language, cover phishing losses.

Some insurers, for example, have taken the position that fake emails do not constitute a fraudulent "entry" or "change" of electronic data required for coverage under certain policies.

Other insurers have denied coverage by arguing that an employee's unwitting wire transfer, made in response to

a fake email, was "authorized."

Insurers have also denied coverage under a forgery policy by claiming that a phishing email is not a "forged" instrument.

Hopefully, common sense will prevail in coverage disputes over phishing and related cyberfrauds.

In the meantime, a knowledgeable, trusted insurance agent can help your business find the most appropriate cyber policy for your company's needs.