HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. October 19, 2015 Volume 1, Issue 10

Serving the Roanoke area since 2006

National Cyber Awareness Month

Spear Phishing

The President of the United States has declared October as National Cyber Awareness Month. So, we are going to talk about Spear Phishing, as opposed to standard Phishing.

Let's differentiate:

Phishing is any fraudulent attempt to extract personal or financial information, through use of email, that appears to come from a legitimate company and is generally sent out en masse hoping for anyone to open it

Spear Phishing is the same type of attack that is targeted at a specific group or company

Generally, the criminal sends an email that appears to be from your bank or credit card company or some other large, well-known business. They steal that company's logos off their website and use them in the email sent to you to help make the email more believeable. If you click on the enclosed link, you may be asked to enter your account number or personal information for "verification" purposes. An enlcosed link may also load spyware or malware to the machine that opens the link.

Spear phishing emails often appear to have been sent by friends, family members and organizations that the target does business with. The emails often contain information that the victim may believe is only known to their close circle of friends.

Information used to convince the target to click on a link or open an attachment is often gained by accessing Social networking websites such as Facebook and Twitter. In some cases, when the victims are particularly well researched and the cybercriminals skilled, it can be very difficult to determine whether a link or attachment is genuine. The "from" field in an email is often masked and made to display the email address of a friend or colleague. The name of the sender can therefore not be trusted.

It can be difficult to spot a phishing email that has been well researched and carefully written, but with a little training speculative phishing campaigns can be easily identified in many cases, provided the recipient is security aware and knows some of the common tell-tale signs that the email is fake.

Helping Your Staff

The advice that all healthcare workers must try to follow at all times, is: **Stop. Think. Connect.**

If suspicions are aroused by a link, attachment or request for information, it is better to delete the email or mark it as junk and seek advice. The golden rule is, **if in doubt do not click**. It is better to delete a suspicious email than to inadvertently give hackers the information they seek or to inadvertently download malware. If the email is important, the sender is likely to make contact again.

Homeland Security offers some useful advice in this regard, and suggests efforts are made to check the legitimacy of an email that requests account information, or a visit an unfamiliar website, namely to:

- Contact the company directly.
- Contact the company using information provided on an account statement or back of a credit card.
- Search for the company online – but not with information provided in the email.

A little information can go a long way. There are tell-tale signs that an email is not genuine and it is important that employees are shown how to recognize potential phishing emails, and are shown how to recognize some of the common identifiers.

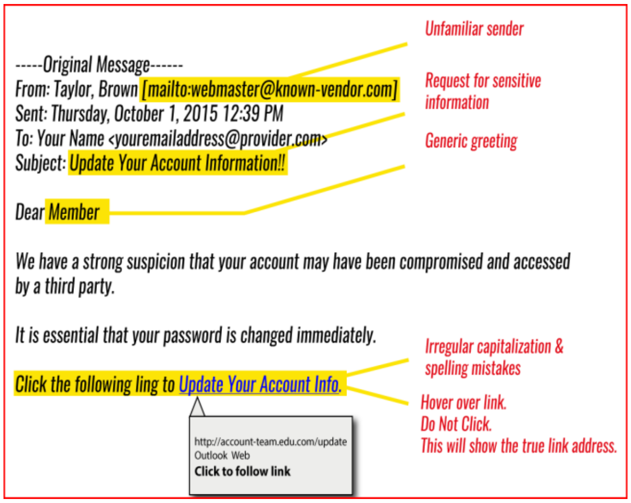
HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. October 19, 2015 Volume 1, Issue 10

Serving the Roanoke area since 2006

How To Spot A Phishing Email

- Requires disclosure of username or password
- Contains links to unfamiliar websites
- Subject lines includes exclamation marks (!!!)
- Urgent call to action – such as must reply within 24 hours
- Explains that there will be dire consequences for inaction
- Contains a generic greeting – Dear Sir
- Contains spelling errors, poor grammar
- No contact information supplied
- Contains foreign characters/symbols



-----Original Message------
From: Taylor, Brown [mailto:webmaster@known-vendor.com]
Sent: Thursday, October 1, 2015 12:39 PM
To: Your Name <youremailaddress@provider.com>
Subject: Update Your Account Information!!

Dear Member

We have a strong suspicion that your account may have been compromised and accessed by a third party.

It is essential that your password is changed immediately.

Click the following ling to Update Your Account Info.

http://account-team.edu.com/update
Outlook Web
Click to follow link

Unfamiliar sender
Request for sensitive information
Generic greeting
Irregular capitalization & spelling mistakes
Hover over link. Do Not Click. This will show the true link address.

COMPUTER NETWORKS OF ROANOKE, INC
www.computernetworksroanoke.com
866-783-5195 EXT. 232

HIPAA COMPLIANCE AUDITS ROUND TWO

"Organizations must complete a comprehensive Risk Analysis and establish strong Policies and Procedures to protect patients' health information," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

SecurityMetrics, a Utah-based merchant data security and compliance company, conducted a survey of health IT professionals to gain a better understanding of the general state of HIPAA compliance among healthcare organizations.

Their survey was on the attitudes on common patient health data protection issues, network security measures used to safeguard data, and other security issues such as Wi-Fi encryption. The aim was to gain a better understanding of the efforts U.S. healthcare organizations are making to comply with the HIPAA Security Rule.

Over 300 healthcare professionals took part in the survey and were asked over 40 questions relating to data security and patient privacy issues, as well as being asked to rate their own organization's compliance efforts. The company's report provides some insight into the general state of HIPAA compliance. Some of the key findings of the report have been listed below:

- 10% of respondents indicated their organization did not plan to achieve full HIPAA-compliance status
- 20% of C-Suite staff did not plan to follow all HIPAA Regulations
- 77% of Organizations provided Security Rule and Privacy Rule training to staff, yet, to 10% said their staff received no HIPAA training whatsoever.

- 60% of compliance officers and health IT professionals said their organization had developed a Risk Management Plan
- Only 63% of healthcare organizations were currently encrypting Protected Health Information stored on work devices
- Confidence in compliance efforts was high, with 80% believing their organization was HIPAA-compliant, although only 76% of risk and compliance officers believed that their organization would actually pass an OCR HIPAA-compliance audit.
- Most of the IT professionals' and compliance officers' answers revealed their organizations were not actually fully compliant with all aspects of the HIPAA Security Rule.

According to SecurityMetrics HIPAA Security Analyst, Brand Barney, ***"The healthcare industry is significantly less secure than executives think."***

Fortunately, with at least two and a half months to go until the second round of HIPAA-compliance audits start, there is still time for healthcare organizations to address risks and achieve full compliance status. Based on the results of the surveys, a small percentage plan to do very little. For those companies, if they are selected for an audit, they could be in for a rude awakening, and potentially a very costly one. If they escape an audit, the next data breach suffered could still see considerable costs incurred.

SecurityMetrics pointed out that in addition to an OCR HIPAA fine of up to $1.5 million, per violation category, per year, the costs that could potentially be incurred include:

- State attorneys general fines in the region of $150,000-$6.8 million
- Federal Trade Commission Fines of $16,000 per violation
- Credit monitoring services for data breach victims at $10 per individual
- Approximately $1,000 per breach victim if a class-action data breach lawsuit is successful
- Loss of patients – Which could be as high as 40%

We have a Network Administration client that we quoted last year on a Security Risk Analysis. They declined the quote because they felt that the price was too high.

Subsequently, they have been audited by CMS, and it appears that they may have to return $132,000.00 in ARRA Stimulus money to the government.

While I am not at liberty to discuss specifics, I can tell you that they would not have paid us anywhere near $132,000.00 for a Security Risk Analysis. Which means that paying us to conduct your SRA in order to keep your Stimulus money, turns out not to be such a bad deal after all.

Have *You* Committed Medicare Fraud?

Folks, you were supposed to have conducted your first HIPAA Security Risk Analysis in 2005 to identify problems in your organization related to protecting electronic Protected Health Information (ePHI).

If you attested to Meaningful Use without having conducted a proper Security Risk Analysis, and without having remediated the problems found, you have most likely committed Medicare Fraud since you took money from CMS as part of the American Recovery and Reinvestment ACT (ARRA).

If you think that might be the case, then it is time to step up to the table and get your Practice compliant BEFORE the folks at OCR show up.

A **Security Risk Analysis** is *required* for compliance. Call us today if you have not done yours or have questions about the process.

Hank Wagner, Owner
757-333-3299 x232
hank.wagner@computernetworksinc.com

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. October 19, 2015 Volume 1, Issue 10

Serving the Roanoke area since 2006

NEW! 36 Month HIPAA Compliance Plan

36 months of HIPAA compliance consulting (includes a complete, onsite, Security Risk Analysis with Remediation Plan, quarterly network scans for 3 years, Policy and Procedure templates including guidance on implementing, incident investigation, breach investigations, unlimited HIPAA compliance questions) for one low monthly fee. Ask, call, or email me for details!

PHI is everywhere. Find it. Protect it.

My Doctor's Business Is Too Small To Worry About HIPAA Compliance

What color is the sky on the planet you are from?

The sad thing is that a Practice Administrator said this to me in a meeting not too long ago. Folks, your size does NOT MATTER. Your lack of protection of ePHI (electronic Protected Health Information) is what matters.

If you have failed to secure your Practice from the threats that come from the Internet using current hardware and software, failed to train your staff on how to identify those threats, failed to regulate access to your corporate network from Vendors, Staff and others, allowed your Patients to use your corporate WiFi and generally thumbed your nose at HIPAA compliance because you do not think you will be a target, then you are completely off base.

The medical record of your patient is worth between $50 and $100 on the Internet. Multiply that number times the number of patients in your database and the next thing you know, you have some data that is worth a LOT of money to the crooks. Let me help you with the math:

Let's use the $50 number x 2,000 patients. That equals $100,000.00. Still think you are too small of a target?

These records are being used for identity theft. Why would someone want to do this?

- change identity to commit crimes
- filing of false income tax returns
- obtaining credit in your patient's name
- rent a place to live
- open phone service for criminal activity
- obtain driver's license and other official identification
- apply for Medicare/Medicaid/Health Insurance benefits
- obtain prescription drugs for street sale

So, don't tell me your business is "too small" to worry about compliance. Every medical office is required to comply with HIPAA should be taking all steps necessary to comply.

If you have a CMS audit, which triggers an OCR (Office for Civil Rights) audit, which triggers a State Attorney General audit, which triggers a FTC (Federal Trade Commission) audit, you are going to be writing checks to pay fines, like you were handing out candy on Halloween. How happy will that make **your** Doctor?