

Sharp HealthCare's 2018 Compliance Education

**Staying Vigilant Against Today's
Cybersecurity Threats**

Information Security Module 4



Ripped from the Headlines



In 2015 and 2016, the healthcare industry was a major target for attack.

DEC 31, 2015 @ 09:13 PM 41,592 Free Issues of Forbes

Data Breaches In Healthcare Totaled Over 112 Million Records In 2015

Ad closed by Google
Report this ad
AdChoices

Dan Munro, CONTRIBUTOR
I write about the intersection of healthcare innovation and policy. FULL BIO

TWEET THIS

- According to OCR, there were 253 healthcare breaches that affected 500 individuals or more with a combined loss of over 112 million records.
- The top 10 data breaches alone accounted for just over 111 million records that were lost, stolen or inappropriately disclosed.

ITRC reports 377 health care data breaches in 2016

Jan 31, 2017 - 00:50 PM

The number of U.S. data breaches tracked in 2016 hit a record 1,093, including 377 incidents in the health care and medical field, according to a recent report by the Identity Theft Resource Center. Hacking/skimming/phishing attacks were the leading cause of data breach incidents for the eighth consecutive year, accounting for more than half of breaches reported in the business, educational, health care, government/military and financial sectors, the organization said. ITRC compiles a list of data breaches confirmed by media sources or notification lists from state agencies. It defines a breach as an event in which an individual's name plus social security number, driver's license number, medical or financial record or credit/debit card is potentially put at risk, either in electronic or paper format.

Ransomware accounted for 72% of healthcare malware attacks in 2016

Two new reports from Symantec and Verizon say hackers are using ransomware and phishing attacks to target the industry.

By **Jessica Davis** | April 27, 2017 | 08:54 AM

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Articles 1, Section 8, Clause 8; Article 202; Article 228 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, weapons and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography. Spam messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your
In the payment form and press OK if you have several codes, enter them one after the other and press

In 2017, the trend intensified.

RANSOMWARE ATTACKS RISE 250 PERCENT IN 2017, HITTING U.S. HARDEST

BY ANTHONY CUTHBERTSON ON 5/23/17 AT 1:37 PM

Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.) You can try to decrypt some of your files for free. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to pay.

Payment will be raised on 5/15/2017 16:25:02
Time Left 02:23:58:28

Your files will be lost on 5/15/2017 16:25:02
Time Left 06:23:58:28

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?
Send \$300 worth of bitcoin to this address: 15zGz2CTyp6eCjDkE3DypcXj8QWR6V1

HEALTH IT
Analysis: Healthcare ransomware attacks increased 89% from 2016 to 2017

By ERIN DIETSCH
Post a comment: Jan 7, 2018 at 5:00 PM

Lawsuits frequently follow the announcement of a major breach.

2017 DATA BREACH REPORT FINDS PHISHING, EMAIL ATTACKS STILL POTENT

Paul Roberts
Last Updated: Wednesday July 26, 2017

Healthcare breaches involving ransomware increase year-over-year

Free CISSP Exam Study Guide! Get expert advice that will help you pass the CISSP exam: sample questions, summaries of all 8 CISSP domains and more!

2017 has been a very challenging year for healthcare institutions as these organizations remain under sustained attack by cybercriminals that continue to target their networks.



Responding to Today's Cybersecurity Threats

We all have a responsibility to protect Sharp's data, including:

- Protected health information (PHI)
- Personally identifiable information (PII) and
- Financial information, such as credit card or bank account information

However, the bad guys have stepped up their efforts to steal this valuable information.

How can you play a part in protecting patient data?



Stay Vigilant and Alert

Everyday, you can make good choices so as to protect our patients' data and keep Sharp secure.

We all must stay alert to common threats that can lead to a compromise or breach such as:

- Responding to phishing emails
- Unintentional disclosures
- Mobile device loss and theft

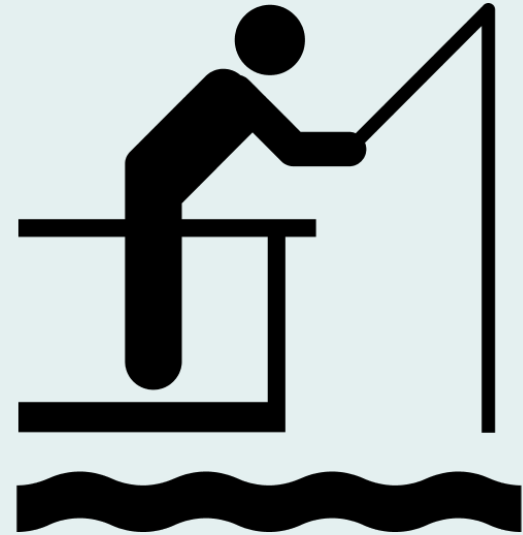
What can **you** do to avoid being compromised?



Be Alert to Phishing Scams

Phishing (pronounced “fishing”) is a social engineering scam often used to steal information.

It typically involves an email and phony websites that trick you into sharing sensitive information such as your user ID, password, or financial information.



Phishing is very often the first step in breaching an organization's defenses.

Be Alert to Phishing Scams

Phishing attacks are becoming more and more sophisticated

- At first glance, an email or website may look legitimate.
- An email may even appear to be from someone you know.
- As a result, people are easily tricked and fall victim to the scam.



How can you avoid becoming a victim of phishing?

Learn How to Recognize Phishing Attempts

Please take a moment to review the tips below to protect you and Sharp from the next suspicious email.

Sender: Jane.Doe@sharp.com

A check of the Outlook Address Book indicates the Sender is NOT a member of Sharp's Information Systems Department

Not addressed to an individual

Dear Webmail user,

Your password as expired. You are hereby directed to click on [ITS HELPDESK/CHANGE PASSWORD](http://unknownORSuspicious.com) to reset your password immediately. Failure to comply with this directives may lead to lose of access to your webmail account. Be warned!!!

Thanks

A scary demand for immediate action!

Poor spelling and grammar

ITS HELP DESK
PASSWORD TEAM

Misspelling and did not come from Sharp's Technical Assistance Center (TAC). There is no contact information for questions or concerns.

Clues on How to Spot a Fraudulent Email:

- An unknown/unexpected or suspicious sender—all external senders will be tagged **[External Sender]**
- Appears to come from a legitimate organization, but the “From” sender address does not match the organization or department
- Not personalized to a specific recipient
- Suspicious or urgent content
- Asks for sensitive information such as Sharp login credentials
- Poor spelling or grammar
- Suspicious links or attachments

Additional Signs of Phishing

Pay careful attention to any website links in emails as an indication of phishing.

IT Scheduled Maintenance – Tuesday, January 19th - 2016

Who is impacted: All staff/User

Description: Mailbox Maintenance Schedule

We have detected that you are using an outdated version of your Outlook Web Mailbox. While your data is still secure within the Portal, This exposes you to other serious security vulnerabilities, and also may cause certain features not to function or display correctly. We strongly recommend upgrading your Outlook Web Mailbox to 2016 at this time.

[Click Here to Upgrade Now](#)

Embedded
website link

Mail Service Team.

Additional Signs of Phishing

By hovering your mouse over the link, you can see that this is a suspicious website.

Do not click!

is still secure within the Portal, This exposes you to other
cause certain features not to function or display correctly
Outlook Web Mailbox to 2016 at this time.

[Click Here to Upgrade Now](#)

Mail Service Team.



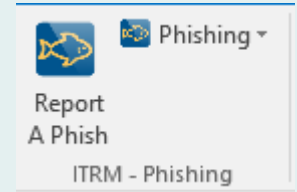
http://owax2.jimdo.com/

**Warning!
Don't Click!!**

How to Respond to a Phishing Email

Suggested Actions:

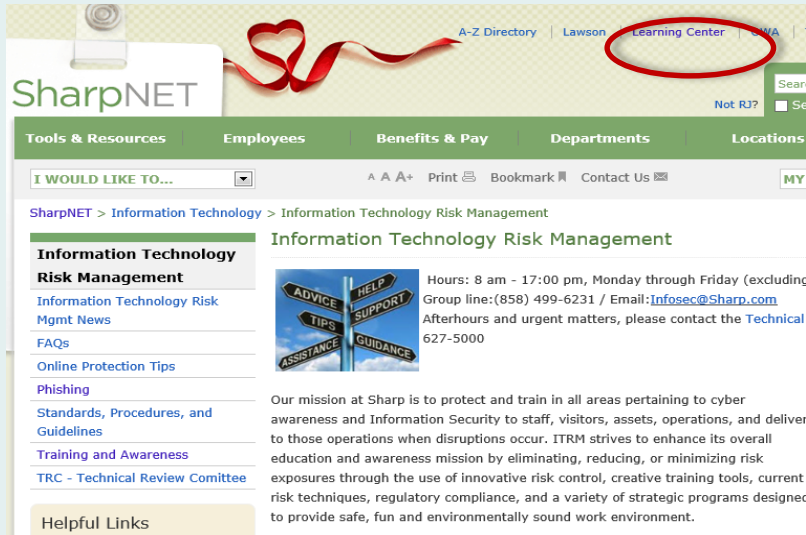
If you are using Microsoft Outlook 2016, you have a “Report A Phish” button installed on your quick access toolbar. Simply highlight the suspected phishing email in your inbox and click the “Report A Phish” button and it will be sent to our IT Risk Management team.



If you don't have the button installed, you should still forward the email in question to the Information Technology Risk Management (ITRM) team at: phishing@sharp.com. Highlight the message in your inbox, then press **CTRL + ALT + F**. This will send the email to ITRM as an attachment complete with headers so that we can do a thorough investigation into the matter and take any corrective actions necessary.

Additional Security Tips

For more information on how to evaluate and respond to phishing, please the IT Risk Management page on SharpNET.



The screenshot shows the SharpNET website interface. At the top, there is a navigation bar with links for 'A-Z Directory', 'Lawson', 'Learning Center', and 'OWA'. The 'Learning Center' link is circled in red. Below the navigation bar, there is a search bar and a 'Not RJ?' button. The main content area is titled 'Information Technology Risk Management' and includes a sidebar with links for 'Information Technology Risk Management', 'Information Technology Risk Mgmt News', 'FAQs', 'Online Protection Tips', 'Phishing', 'Standards, Procedures, and Guidelines', 'Training and Awareness', and 'TRC - Technical Review Committee'. The main content area also includes a 'Helpful Links' section and a 'Hours' section for the Information Technology Risk Management team.

For more in depth training log into the learning center on Sharpnet and search ITRM. We have compiled 29 new modules to help Sharp employees protect information both at work and at home.



Topics Include:

Phishing, Ransomware, Email Security, Travel Security, Web Browsing, Social Networking, and much, much more.....

Unintentional Disclosures

An unintentional disclosure occurs when a well-intentioned Sharp employee mishandles sensitive information by:

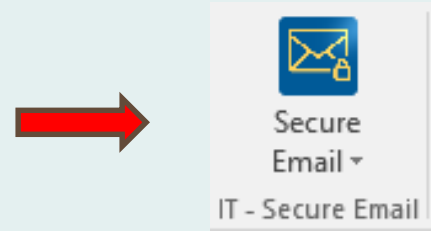
1. Sending sensitive information unencrypted or to the wrong email recipient
2. Sending sensitive information without knowing it was included in the email or within an attachment (e.g. hidden rows or columns in spreadsheets)
3. Allowing your computer screen or mobile device to be seen by unauthorized individuals while you have sensitive information displayed



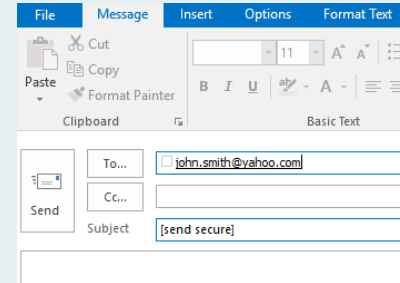
Unintentional Disclosures

Suggested Actions:

If you are using Microsoft Outlook 2016, you have a “Secure Email” button installed on your quick access toolbar. Simply compose your email as you normally would then just click the “Secure Email” button and your email will be sent encrypted to the recipient. **Note:** This button only encrypts emails leaving the Sharp network to external recipients.



If you don't have the button installed, or you are using the Outlook Web Application (OWA) version, you can still send emails securely by typing **[send secure]** in the subject line of the email. Just as with the “Secure Email” button, only emails leaving the Sharp network will be encrypted using this method.

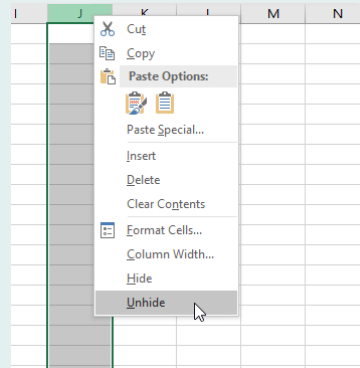


Unintentional Disclosures

Suggested Actions:

Always double check documents you are sending via email to ensure they only contain information needed by the recipient for a valid business reason.

“Unhide” columns and rows in spreadsheets and templates to validate there isn’t residual / hidden data that isn’t intended to be read by your recipient.



Unintentional Disclosures

Protect your computer screen from being viewed by unauthorized individuals. Never leave sensitive information up on your screen when you walk away.

To lock your screen quickly, simply press the Windows logo key and “L” at the same time and your screen will lock.



If you don't have a Windows logo key on your keyboard, press Ctrl + Alt + Delete simultaneously and you can select to lock your screen manually.



Protect Your Mobile Devices

Mobile devices are transforming how we interact with our patients and business partners. If proper precautions are not taken, it could potentially result in exposing sensitive information.



- Laptops
- Mobile Phones
- Tablets



Personal mobile devices that will store Sharp data and use Sharp resources must get prior authorization.

What are some ways to reduce the risk of exposure when using a mobile device?

Portable Clinical Devices



Clinical devices often use a mobile platform (laptop/tablet) to run the device's software.

These mobile platforms should be reviewed by Sharp's Technology Review Committee (TRC) before being used in our facilities to ensure they have minimum security safeguards enabled.

You should also ensure they are physically secured so as to prevent theft or accidental loss.

TRC Information: <http://sharpnet.sharp.com/is/informationSecurity/TRC.cfm>

Additional Guidance for Personal Mobile Devices

Here are some additional tips to help secure your personal devices and minimize the risk of theft or loss:

- Never leave your personal device unattended
- Password-protect your personal device with a PIN
- Configure the lock screen feature to come on after a short period of inactivity
- Keep your mobile device software up to date



Need More Help?

Please contact the Technical Assistance Center at (858) 627-5000 if you experience the following:

- Lose your mobile device with Sharp data
- Click or open something malicious
- Fear your computer is infected with a virus



If you have any questions or concerns related to information security, please contact IT Risk Management at infosecgroup@sharp.com

Exit Instructions:

We hope this course has been informative and helpful.



Next Steps:

Click on the “X” (close button) in the upper right hand corner of the screen when you are ready to complete the requirements for this course.