Annual Information Security Training

Overview

This training will enhance your understanding of the goals of the Rady Children's Information Security Program and our collective responsibilities regarding risks to the organization, patient and personal data, and more.

Learning Objectives

Upon completion of this module, learner should be able to:

- Describe the impacts of data security incidents.
- Recognize and employ available tools and strategies to protect data.
- Identify the common types of social engineering and how to avoid them.
- Comply with EPM 13-07, Password Management.
- Describe the negative impacts of Ransomware on healthcare organizations.
- Apply best practice strategies to defend against data security breaches.
- Identify and utilize available resources to report data security concerns.

Cyber Safety is Patient Safety

You play a key role!

Impacts To Healthcare

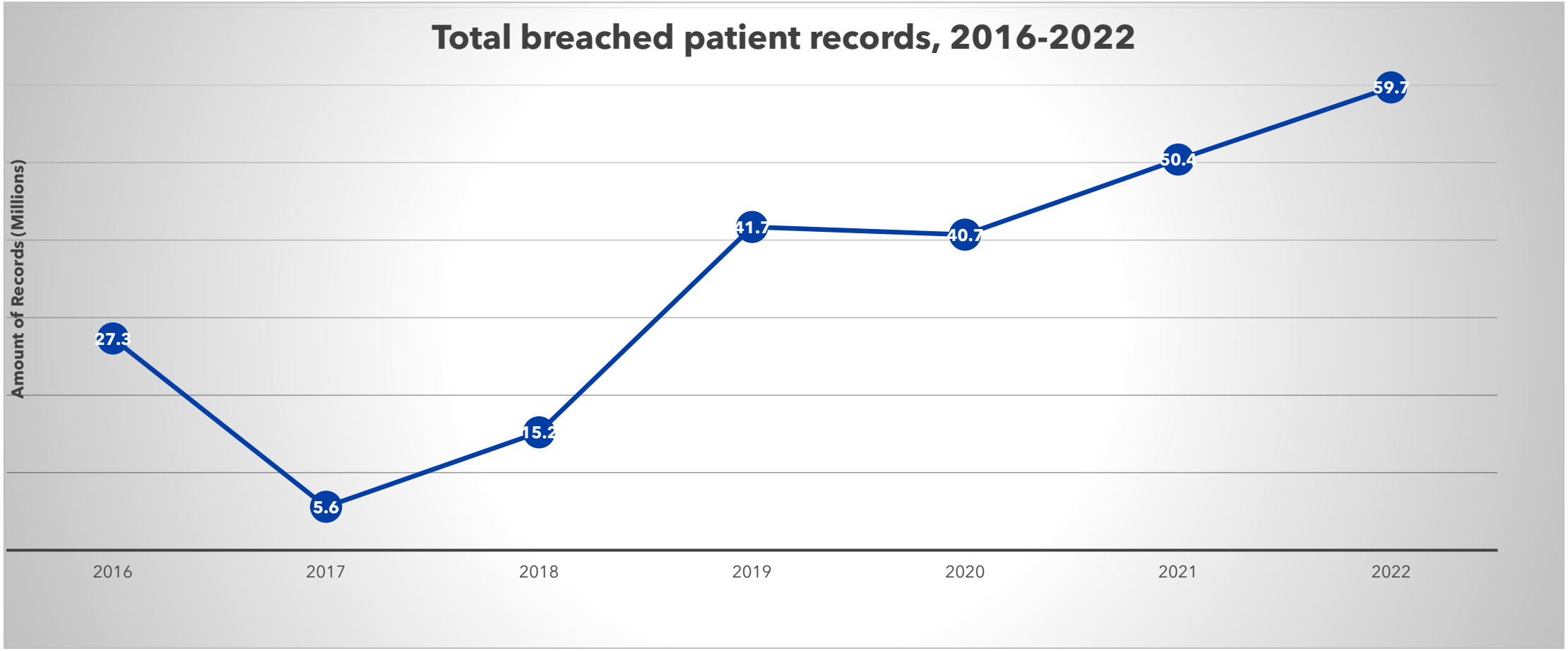
$10.10 Million

Average total cost of a breach in healthcare

- Hacking was responsible for 75% of all reported incidents in 2022.
- Hacking incidents include phishing/email attached and ransomware/malware incidents.
- 86% of all breached patient records in 2022 were caused by hacking!
- **1 medical record** sells for **$250!**

The number of patient records compromised in data breaches is up 46% from just two years ago.

BreachBarometer 2022



HIPAA and the Security Rule

- Covered entities are required to adhere to U.S. Department of Health and Human Services (HHS) developed regulations protecting the security of health information.
- These Regulations form the security rule, which establish national standards to protect Protected Health Information (PHI).
- Appropriate security controls are required to ensure the following is applied to all PHI.
  - **Confidentiality** – Ensuring information is not improperly disclosed.
  - **Integrity** – Ensuring data is accurate, complete, and has not been altered in an unauthorized manner.
  - **Availability** – Systems are accessible upon demand by those authorized to use them to help care for our patients.

Data Security: Data Encryption

- HIPAA requires PHI be encrypted in motion and in storage:
  - USB drives must be encrypted utilizing approved RCH methods/standards.
  - Storage on unauthorized platforms/devices poses significant risk to RCH.
- EPM 13-12 Storage Media Protection

Data Security: Unauthorized Disclosure

- Never leave devices unattended in open areas such as cars, restaurants or waiting rooms
- Never leave printed documents containing sensitive information unsecured or within public view (i.e. unattended printers or fax machines)
- Never leave your computer monitor open towards public view when sensitive information is being displayed
- Report suspected HIPAA violations to the **R**eal **L**earning for **S**afety (RLS)

"An insider threat in the Healthcare and Public Health (HPH) Sector is potentially a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems."

– Department of Health & Human Services, 4/21/22

Insider Threats Defined: Who, What, Why?

- Involve people in the organization who have legitimate access to your computer systems and network.
- Negligence or malice causes these insiders to compromise your patient and enterprise data.
- Repercussions can occur for patients, security and overall quality of care.

- Accidental Insider Threat
  - Honest mistake
  - An example would be a phishing email containing an embedded link, which then sends the email information to an unknown source.
- Intentional Insider Threat
  - Malicious loss or theft to organization network, infrastructure or database with an objective of personal gain or inflicting harm to a person or the organization.

Insider Threats

Insider threats have increased across all three insider profiles:

- Careless or negligent employee or subcontractor
- Criminal or malicious insider
- Credentialed thief

Careless or negligent employees equal 56% of the incidents.

Who is Behind Insider Threats?

An engineer steals and sells trade secrets to a competitor

A maintenance technician cuts network server wires and starts a fire, sabotaging operations

An intern unknowingly installs malware

A customer service representative downloads client contact information and emails it to a personal account for use when starting their own business

A database administrator accesses client financial information and sells it on the dark web

How Could This Happen?

61% of data breaches involving an insider are primarily unintentional and caused by negligent insiders

Lack of awareness of security policies and training

Leaving an unencrypted mobile device or laptop containing sensitive data unattended, leaving the potential for loss or theft

Employee grievance against the organization

Six Reasons to Protect Healthcare Data

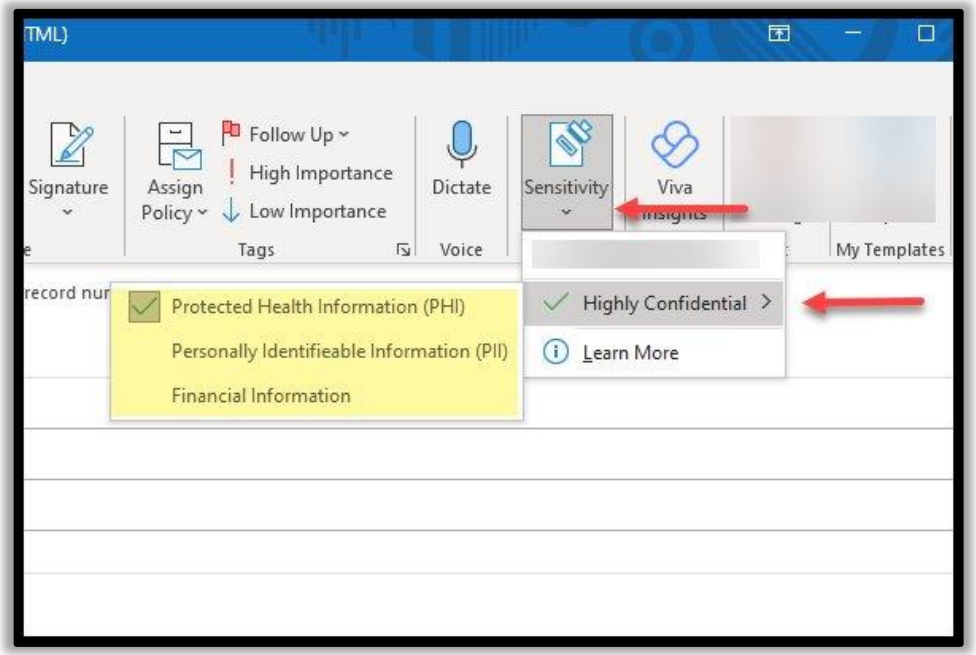
- Transmission of sensitive data –PII/PHI
- Sensitive data comprises the majority of your day-to-day duties.
- PHI is discussed, stored, processed and transmitted between information systems daily.
- Protecting sensitive data requires robust policies, processes and technologies.
- Impacts to the organization can be profound if data are corrupted, lost or stolen.
- Security breaches may prevent users from completing their work on time and adversely impact patient care.

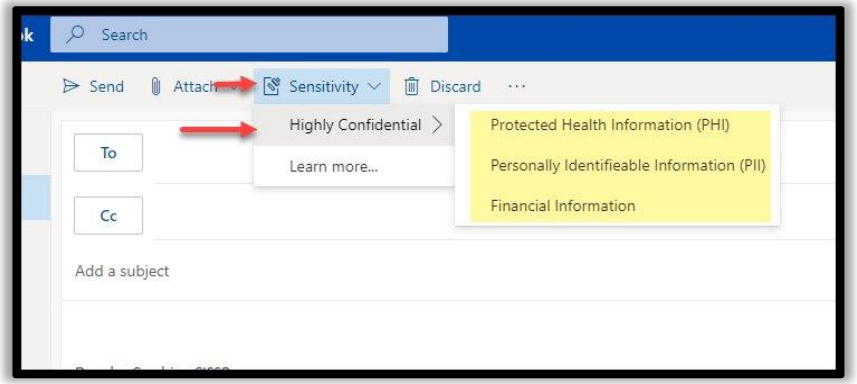
Steps to Protect Your Data

- Do not plug an unknown USB drive into your computer.
- Keep personal and business USB drives separate.
- Use and maintain security software and keep all software up to date.
- Always maintain physical control of mobile devices including cell phones, tablets, portable drives, etc.
- Avoid storing PHI or other sensitive information on mobile devices.
- Ensure that mobile devices, such as iOS and Android phones or tablets, are authorized to access RCH email are configured with Mobile Device Manager (MDM).
- If you suspect that an MDM enabled device has been lost or stolen, report it immediately to the Service Desk.
- EPM 13-04 Mobile Device Security

Data Security: Email Encryption

If you need to email PHI or sensitive information, you must encrypt your message with a sensitivity label.





Important: Before you hit send, make sure your email is only addressed to those you want to send it.

See Something, Say Something

- Follow your instinct and always report what does not look or feel right to you.
- Beware of social engineering techniques.
- Participate in regular security training sessions and if you haven't, speak to your manager or IT Security.
- Be aware of security risks and the associated consequences of failing to comply with organizational policies. Now is the time to know all the rules, not when an incident has happened.

See Something, Say Something

- Don’t be a victim, be proactive!
- Always contact your manager or IT Security if you believe you may be a victim of data loss or have made an honest mistake. Timeliness is key in reporting.
- Every situation will vary so your manager or IT security professionals will be able to guide you best because a cyber threat is not limited to just hacking.

Summary

- Insider threats happen at every organization. They may be accidental or malicious in nature.
- These threats can cost an organization millions of dollars and potentially cause it to shut down.
- See something, Say something. Contact your Manager or IT Security if you believe you are a victim or have made an honest mistake. Swift action can make a difference.

What is Social Engineering? How does it work?

Social engineering is a form of psychological manipulation that tricks users into making security mistakes or giving away sensitive information. It relies on human error instead of vulnerabilities in software and operating systems by exploiting human emotions.

Examples:

- Email sent by a 'friend'
- Message relaying a troubling story about someone you may know
- Message says 'time is running out'
- Offer seems too good to be true
- Message offers help you never requested
- Sender cannot confirm their identity

Human error is much less predictable, making it harder to detect and block than attacks on hardware or software.

Common Clues in Social Engineering

Trick you into:

- Revealing information
- Installing malware
- It relies on human error instead of vulnerabilities in software and operating systems.

What is The Most Common Form of Social Engineering?

Phishing

- A form of Social Engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy organization.

Spear Phishing

- A form of Social Engineering that targets a narrower audience, hence the spear. These attacks are more coordinated.

Phishing Scams Have Similar Traits!

- Contain a call to action – click, open, reply
- Conveys a sense of urgency
- Contains odd aesthetic features, like blurry or overstretched images and misspellings, capitalization, and other grammatical errors

* Remember the definition of social engineering – they are trying to manipulate you into making security mistakes.

Be alert for Smishing attacks

- Smishing is a form of social engineering that exploits SMS, or text messages.
- Text messages can contain links to such things as webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number.
- Users are much more trusting of text messages, so smishing is often lucrative to attackers phishing for credentials, banking information, and private data.

Threat: Social Engineering

- **Social Media** (Facebook, Twitter, Instagram, Message Forums, etc.)
  - Used for information gathering
  - Info can be used to target you or others with a special phish
  - Info can be used to guess your password
  - Be aware of who you accept as 'friends.'

- **Other methods**
  - Pressure tactics to get you to perform inappropriate behaviors
  - Phone is a common method.
  - Ask for a callback name/number.
  - Physically tailgating into a restricted area
  - Validate guest badges and do not allow someone into a restricted area without having them badge in first.

- **Phishing Emails**
  - Designed to look legitimate &/or enticing
  - Don't open attachment(s)
  - Don't click on link/URL (Hover over link to verify)
  - **Let us know if you did click/open!**
  - Forward to IT Security at **phishing@rchsd.org**

Recognizing and Reporting Phishing

What to ask? There are 4 things to check when you suspect an email might be a phishing attempt. If you are ever in doubt, send to phishing@rchsd.org

Sender is Unfamiliar or Unexpected

- Do you recognize the sender?
- Are you expecting a message from this person
- Does the subject seem normal?

Message Doesn't Look Right

- How's the use of English?
- Is everything spelled correctly?
- Is it formatted like a regular email?

Check 'From' Address

- Does it look legitimate
- Double click the 'From' to inspect
- Both should look similar
- CustomerService@amazon should not read "bob@scamyou.org"

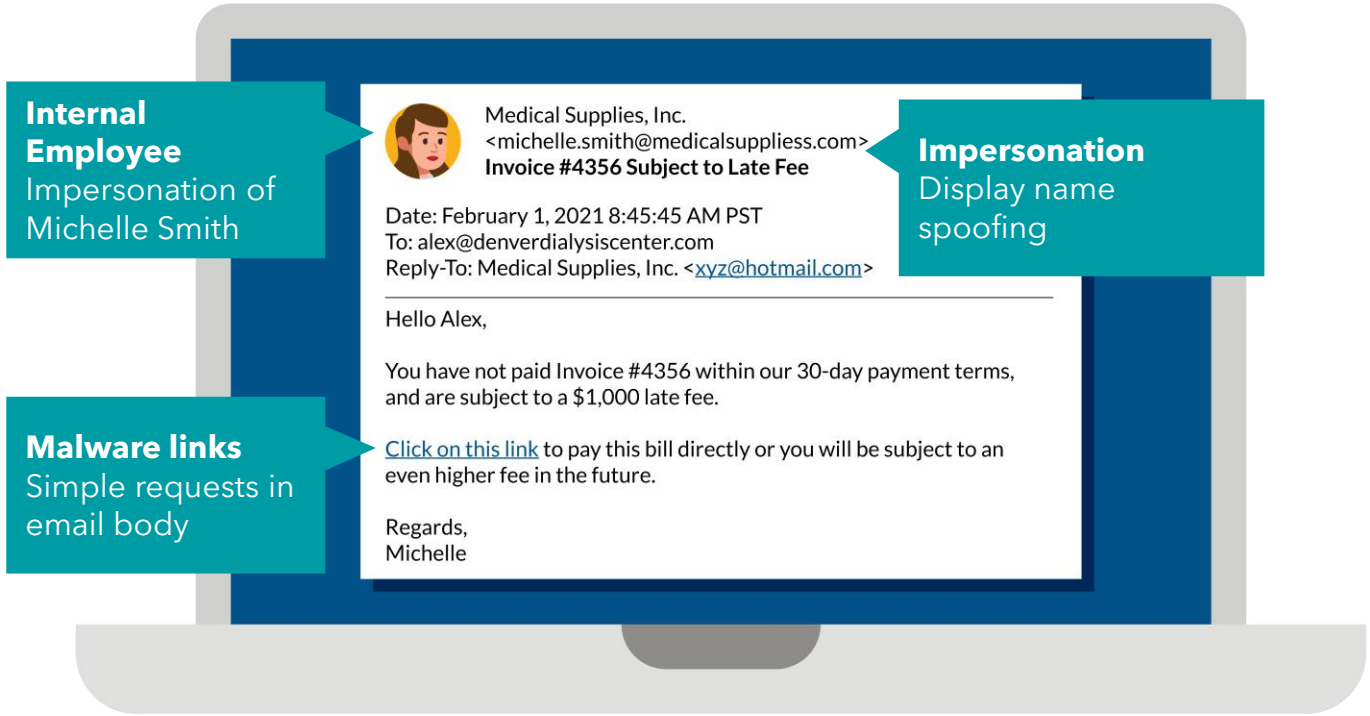
Inspect All Links and Attached Files

- Hover over the link or attachments and ask yourself these questions:
- Does the displayed URL make sense?
- Contact the company directly to confirm they sent the email

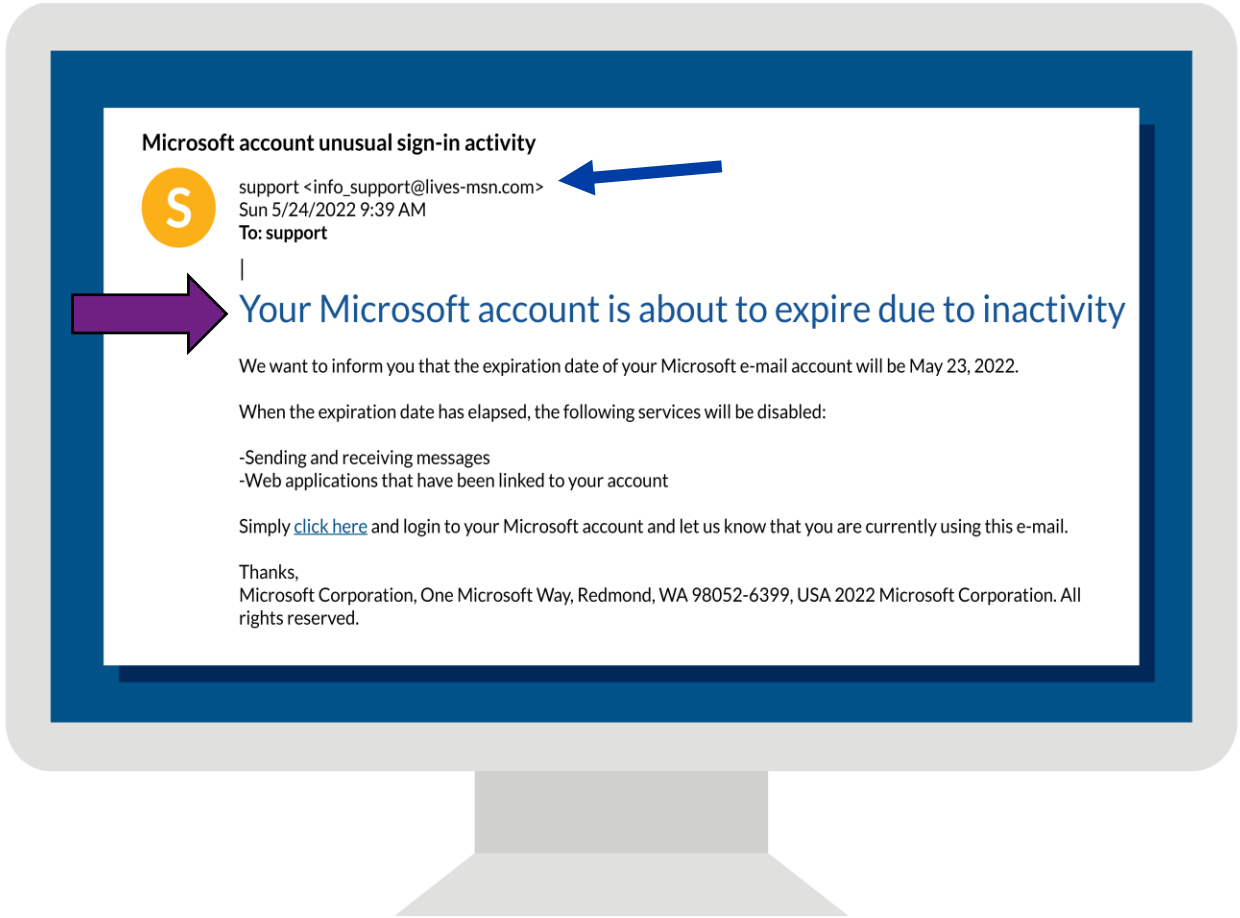
Exercises

- Now, let's look at some "phishy" emails and see if you can spot the red flags!
- Remember, the hackers are trying to trick you, so don't grab that hook!!

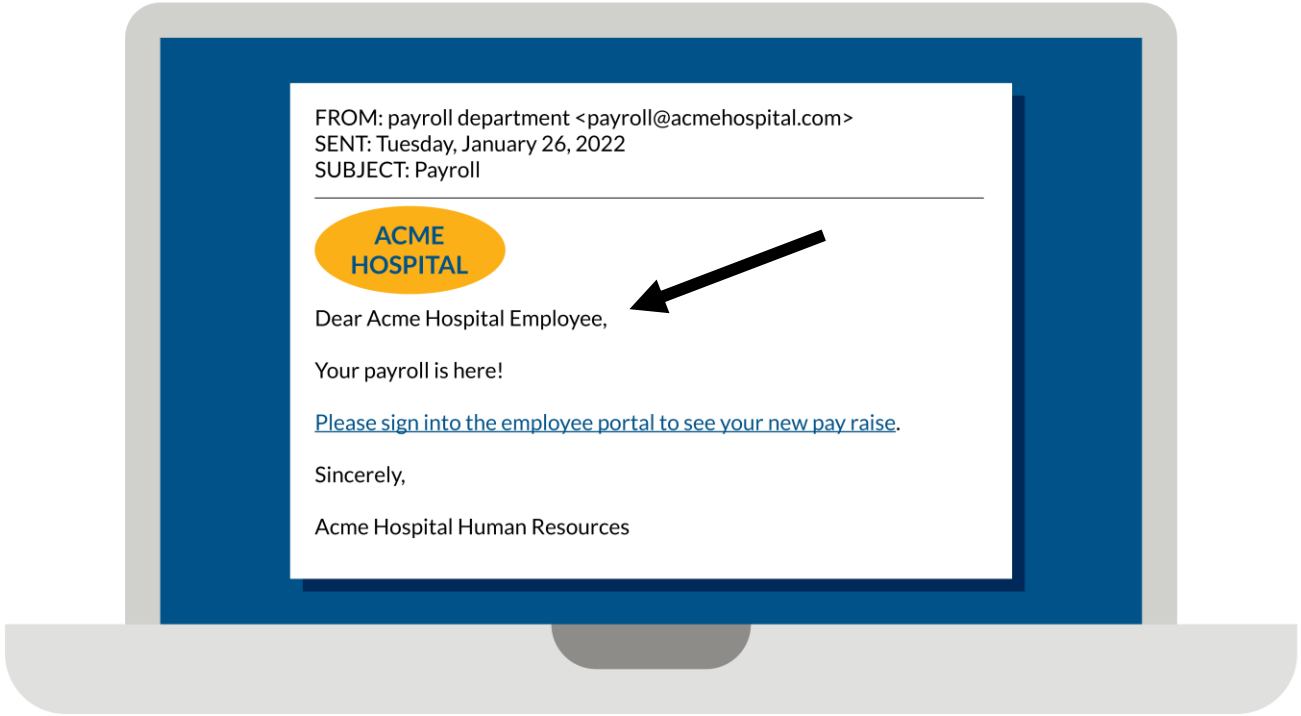
Would you have taken the hook on this email?



Would you have taken the hook on this email?



OK, This is a Simple Request! Pay Raise? Where do I Click?



Phishing Checklist

Check your cyber pulse

- Don’t recognize the sender?
- Not expecting an attachment or email?
- Does ‘From’ address match message?
- Does this invoke a sense of urgency?
- Don’t recognize the destination URL?
- Is this standard internal procedure for IT issues?
- Is this website secure? (http**s**://)
- Is this email asking for your login credentials?
- Is there bad grammar or spelling?
- Is the greeting/signature generic or do they lack contact information?

Example: Social Engineering

Please watch the video below as there is a quiz question!

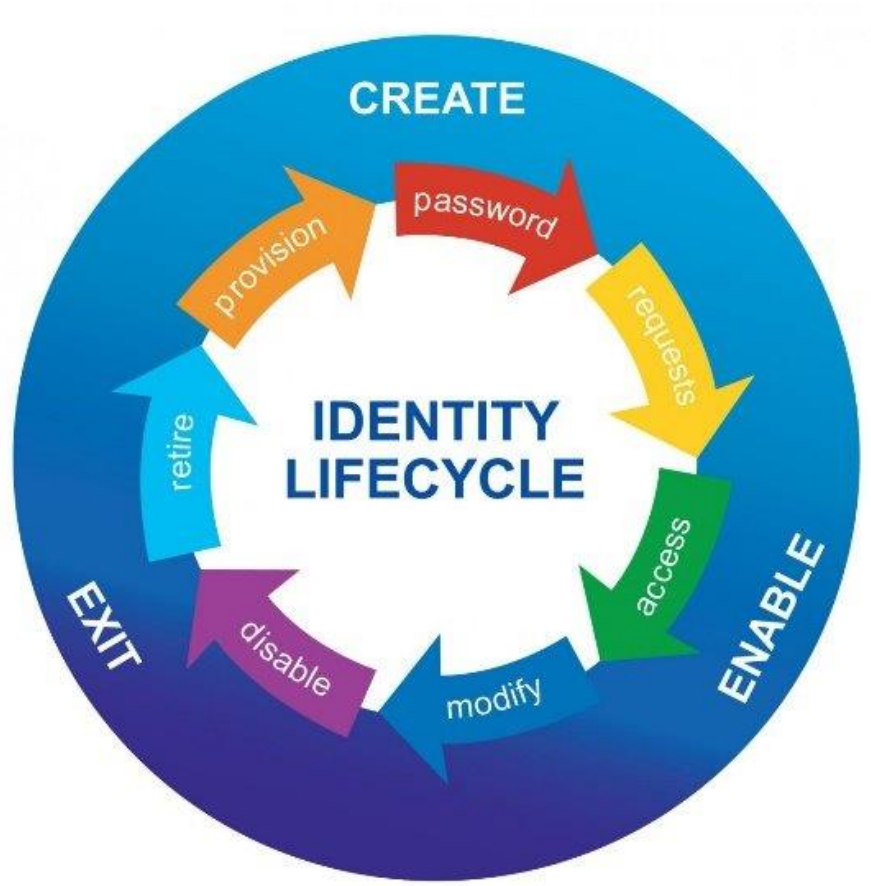
Ocean's 8 Favorite scene - 9 hack into the man's computer - YouTube

Passwords

- Our enterprise policy 13-07 Password Management covers expectations with passwords.
- Passwords should be unique to Rady Children's and each instance (e.g. your network login must be different than your login to another work-related website)
- Your primary account for access is used for access to your computer, Microsoft 365, Citrix, and more. This password should not be used for any other purpose, including other sites that are work related but not tied to your network account.
- For a convenient way to keep track of your work passwords, we offer a password management solution at https://passwords.rchsd.org. This secure platform is available on the network for you to store, access, and manage your various work-related credentials.
  - All users at RCHSD have access and the platform can be used for group access to shared lists as well. For more information, please visit the Success Center and search PasswordState or click here.

Identity Management

- Use strong passwords and commit them to memory.
- Do not accept multi-factor authentication requests that you are not expecting.
- Never use the same password for your work account as for your personal account. Recent compromises on commercial sites (Yahoo, LinkedIn, etc.) have exposed personal passwords!
- ***Do not*** write down passwords or store in unapproved locations.
- We have https://passwords.rchsd.org available for your use to securely store and share passwords.
- Never leave a workstation that is logged in unattended.
- Lock your computer screen by pressing Ctrl-Alt-Delete and selecting 'Lock this computer' whenever you leave a desk or work area and be sure to secure the application you are using (you can also use the WIN-L combination).
- Log off your computer when you leave work each day.



What is Ransomware?

"Ransomware poses a threat to you and your device but what makes this form of malware so special is the word 'ransom'. Ransomware is extortion software that can lock your computer and then demand a ransom for its release."

In simple terms:

- Malware gains access to the device.
- Depending on the type of ransomware, either the entire operating system or individual files are encrypted.
- A ransom is then demanded from the victim.

Ransomware Facts

Ransomware incidents
can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Malicious actors are getting more sophisticated with their tactics, even pressuring victims for payment to stop the release of the stolen data

Ransomware incidents have become more destructive and impactful in nature and scope.

Ransomware demands in most cases exceeded $1 Million Dollars!

Impacts to Healthcare - Facts

FBI IC3 – Internet Crime Complaint Center (IC3) March 2022

"Healthcare Sector Faced Most Ransomware Attacks Last year"

- The IC3 confirmed the Healthcare sector faced the most ransomware attacks in 2021; The FBI pays a lot of attention to the topic of Ransomware.
- 148 complaints files were healthcare Ransomware attacks.
- In 2021, the IC3 observed 847,376 complaints and recorded $6.9 billion in losses. These numbers have been steadily climbing over the last five years.
- Phishing emails remain at the top of the list for initial infection vectors for ransomware.
- Don't get hooked!

"Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally."

Impacts to the Organization

- Monetary impacts to the organization
- Potential impact to the organization's reputation
- Permanent closures of organizations, especially the smaller ones
- Loss or deletion of files
- Delayed or cancelled patient care: procedures, testing, surgery, etc.
- Systems shut down, potentially crippling network systems and forcing manual transactions where possible
- Reportable breaches

What You Can Do!

- Change your passwords when prompted to do so and never share your password!
- Do not accept multifactor prompts that you did not initiate
- Be aware of phishing emails – this is the top choice for an initial cybercriminal attack
- Report incidents or suspicions to your Manager or IT Security

- Hover over the email URL – be sure you know who the sender is – if not report it
- Software updates
- Check your mobile settings to activate QR code confirmation feature
- Preview QR codes before launching

The Best Defense is a Good Offense

Staying Resilient

- Most ransomware attacks are sent in phishing campaign emails.
- Stay alert when any email asks you to enter your credentials.

Self-Check List

- Be on the lookout for any updates you receive from your office administrator or IT administrator. IT Alerts are a good source of information.
- Install updates whenever prompted to do so.
- Are you aware of your unit's downtime procedures?
- Is there training I should be aware of to understand my organization's security policies?
- Do I have an emergency contact list?

Teleworking

- Teleworking requires an approved Telework agreement on file with Human Resources.
- Ensure your workspace is compliant with our clean desk expectations.
- Comply with our Acceptable Use Policies (EPM 13-13 and 11-70).
- If using Citrix on a personal device, ensure it is appropriately secured.
- Avoid connecting to risky and/or public networks.
- If you are traveling internationally and wish to work, this must be cleared by HR and InfoSec.
- We appreciate a heads up if you are accessing email etc. from your phone too!
- See PPM 824 Telework Program and your HR Partner for more information.

Reporting Security Concerns

There are several resources available to you to report security concerns.
Please do not hesitate to reach out if you have questions, suggestions, or concerns:

- Report phishing by forwarding it to ***phishing@rchsd.org***
- Contact Sahan Fernando, Chief Information Security Officer at (858) 576-1700 x246273 or ***mfernando@rchsd.org***
- Report suspected HIPAA security violations to the Real Learning for Safety (RLS) system
- Contact Christina Galbo, Chief Compliance & Privacy Officer at (858) 966-8541 or ***cgalbo@rchsd.org***
- Call the confidential Compliance Hotline at (877) 862- 4228