STEVENS
INSTITUTE OF TECHNOLOGY
1870

Teaching Cybersecurity to Non-Experts

Final Exam 5 (U–Z)

Komal Wavhal

27 Apr 2025

Team Member

Komal Wavhal
CWID: 20034443

Exam Question

Teaching Cybersecurity to Non-Experts

Imagine you've been asked to create a short curriculum to teach non-technical hospital staff the basics of cybersecurity.

Your goal is to explain core concepts without technical jargon, using metaphors, analogies, and real-world examples where possible.

Write an instructional guide that covers:

- What threats and vulnerabilities are (Lecture 1)
- How personal and patient data can be stolen (Lecture 2)
- The importance of passwords, MFA, and authentication (Lecture 3)
- Why phishing works and how to spot it (Lecture 4)
- The basic idea behind encryption (Lectures 6 and 7)

Lecture

1. What threats and vulnerabilities are
2. How personal and patient data can be stolen
3. The importance of passwords, MFA, and authentication
4. Why phishing works and how to spot it
5. Why phishing works and how to spot it
6. The basic idea behind encryption
7. The basic idea behind encryption

Introduction

The objective of this curriculum is not to turn non-technical staff into cybersecurity experts, but to provide them with the knowledge they need to make informed decisions, avoid common pitfalls, and recognize potential security risks in their daily work. As healthcare continues to evolve and become more reliant on digital technologies, the role of every staff member in cybersecurity becomes increasingly important.

In today's increasingly digital world, cybersecurity is a critical concern for all industries, including healthcare. Hospitals and healthcare providers are responsible for safeguarding vast amounts of sensitive information, from personal patient data to medical histories, that could have devastating consequences if compromised. While the complexity of cybersecurity may seem daunting, understanding its basic principles and how they apply to daily operations is essential for all hospital staff, even those without technical backgrounds.

Cybersecurity can seem like a foreign concept to those without an IT background, but the core principles are simple and easy to grasp. Just as we take precautions in our everyday lives to protect our personal belongings (such as locking doors or securing our wallets), hospitals must implement strategies to protect patient data from unauthorized access, theft, or misuse. Staff members play a crucial role in creating a secure environment by recognizing and responding to potential threats.

This curriculum is designed to introduce non-technical hospital staff to the basics of cybersecurity. Using simple language, real-world examples, and analogies, we will explore core concepts such as the importance of safeguarding patient data, understanding vulnerabilities, using strong passwords, and recognizing phishing attempts. By the end of this guide, hospital staff will have a better understanding of the role they play in maintaining cybersecurity and protecting patient privacy, enabling them to contribute to a safer and more secure hospital environment.

Lecture 1: What threats and vulnerabilities are

Cybersecurity:
In the world of cybersecurity, understanding threats and vulnerabilities is essential. These two terms are often used interchangeably, but they have distinct meanings. Let's start by defining them with an analogy that everyone can relate to: your house.

Threats are like burglars or intruders who want to break into your house, steal your valuables, or harm you. In the context of cybersecurity, threats refer to any potential harm or attack that could be inflicted on your system or network. They could come in many forms, including hackers, viruses, or even inside threats from employees.

Vulnerabilities, on the other hand, are the weaknesses in your house—like an unlocked door or a broken window—that make it easier for a burglar to break in. In cybersecurity, vulnerabilities refer to weaknesses or gaps in your system or processes that make it easier for threats to succeed. This could be anything from outdated software, poor passwords, or even employees who are not trained to recognize risks.

Real-World Example:

Consider a hospital system where software has not been updated for several months. If a hacker is aware of an existing vulnerability, they can exploit it to access sensitive patient information or disrupt hospital operations. This is a clear case of a threat taking advantage of a vulnerability.

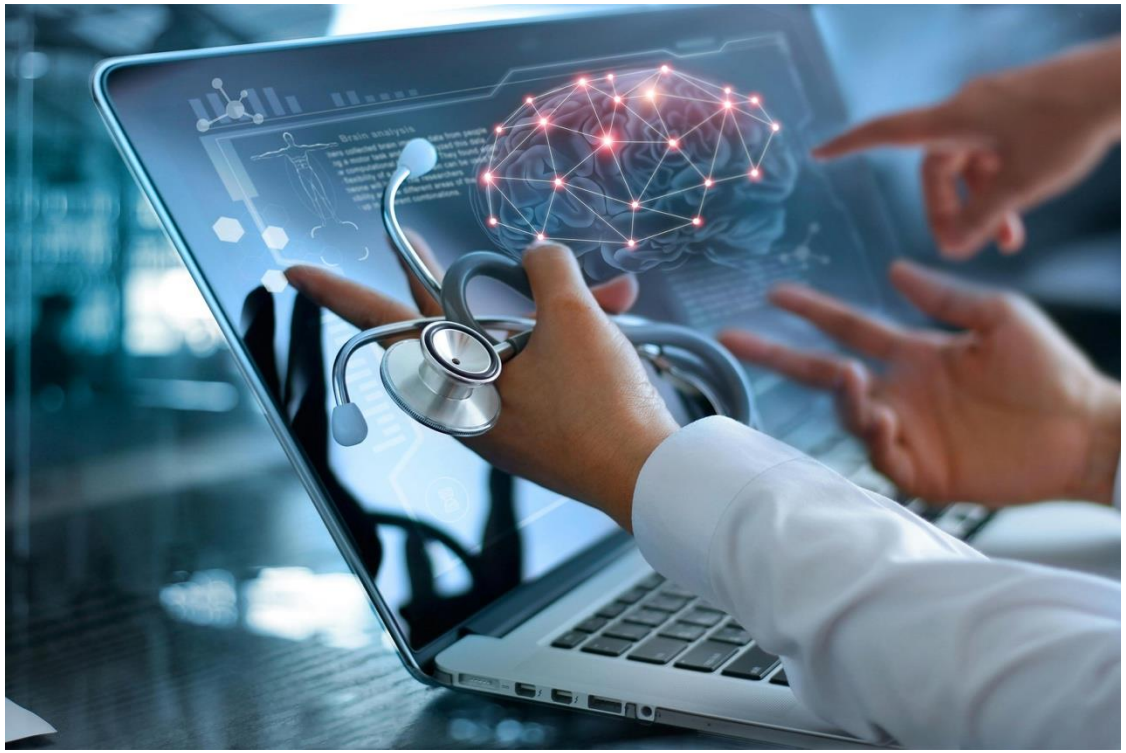
Future Example:

In the future, hospitals might implement more complex systems with interconnected devices, such as smart medical equipment, patient monitoring devices, or cloud storage. Each of these systems could introduce new vulnerabilities, especially if not properly secured. A hacker could exploit a weakness in one of these devices and gain unauthorized access to patient data.

Key Takeaways:

- Threats are potential attacks or harmful actions.
- Vulnerabilities are weaknesses in the system that can be exploited by threats.
- Protecting sensitive information in a hospital setting requires addressing both threats and vulnerabilities through a robust security strategy.

Lecture 2: How personal and patient data can be stolen



Introduction to Data Theft:

Imagine you've written something important on a piece of paper and left it lying around on your desk. If someone walks by, they could easily grab it and use it for malicious purposes. Personal and patient data in a hospital environment works in much the same way—if it's not properly protected, it can be stolen by cybercriminals.

•**Personal Data**: This refers to information about individuals, such as their name, address, date of birth, and other identifying details.

•**Patient Data**: This is more specific and includes health-related information, such as medical history, treatment plans, medications, and test results.

In a hospital, both types of data are extremely valuable. Cybercriminals often target this data because it can be sold on the black market or used for fraud.

How Data is Stolen: There are many ways that hackers can steal personal and patient data:

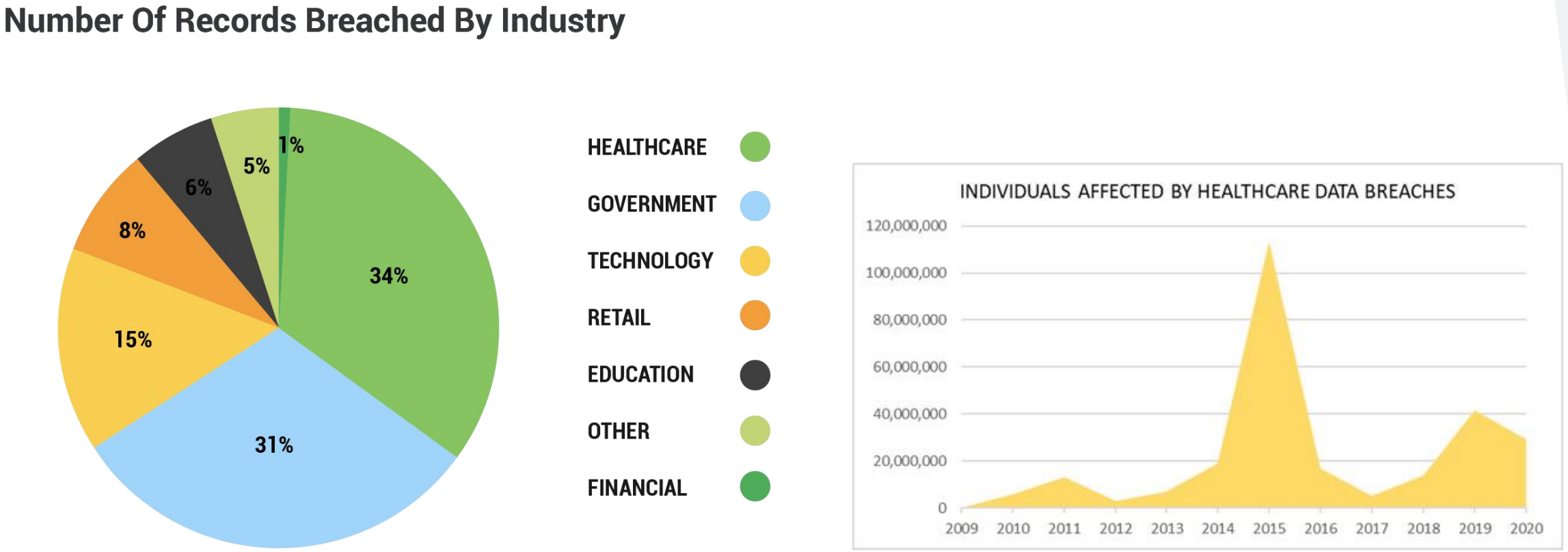
1.Phishing: A hacker might send an email that looks legitimate, asking you to click on a link or provide personal details. If you click, the hacker can gain access to your data.

1.Malware: Malware is software designed to harm your computer. If a staff member opens a malicious attachment or visits a compromised website, malware can infect the hospital's systems and give cybercriminals access to sensitive data.

Social Engineering: This is when hackers manipulate people into revealing confidential information. For example, a hacker might call a hospital employee pretending to be an IT technician and ask for a password or system access.

Healthcare Data Breaches

Real Example: A major healthcare provider in the U.S. suffered a breach where personal and patient data was stolen after an employee fell victim to a phishing attack. The hacker was able to gain access to sensitive information, which included names, social security numbers, and medical records.



Examples of Healthcare Data Breaches

https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

Sr. No	Name	Date	Impact	Description	What was compromised	Learn from this data breach
1	Tricare Data Breach	September 2011	5 million patients	Tricare, a healthcare program for military members and their families, suffered a major data breach after backup tapes of health records were stolen from a transporter's car. It's unclear if the thieves could access the data, but the incident was treated as a breach.	Social security numbers Names Addresses Phone numbers Personal health data Clinical notes Lab tests Prescription information	Though the data on these backup tapes was encrypted, the encryption method did not align with a particular federal standard. To dampen the impact of data breaches reported to HIPAA, a data encryption policy that aligns with federal standards should be implemented.
2	Community Health Systems Data Breach	April-June 2014	4.5 million patients	Cybercriminals, likely based in China, exploited a software flaw with advanced malware, stealing sensitive patient data from the Community Health System network, affecting patients from the past five years.	Names Birth dates Social Security numbers Phone numbers Addresses	Teach employees to recognize the warning signs of malware injection attempts and other cyber threats common to healthcare. Remediate vulnerabilities commonly abused during malware attacks. Regularly refer to the CVE database to remain informed about zero-day exploits impacting popular software solutions.
3	UCLA Health Data Breach	July 2015	4.5 million patients	UCLA experienced a data breach beginning in 2014, with a confirmed cyberattack compromising patient data in May 2015.	Names Dates of birth Social security numbers Medicaid Health plan identification numbers Some medical data	UCLA health was issued with a $7.5 million fine for its failure to report the breach in a timely manner, a violation of the breach notification protocol specified under HIPAA. To prevent such breach reporting delays, it's important to commit to a thorough investigation whenever suspicious network activity is detected.

Future Example:

With the increasing use of wearable health devices (like smartwatches that track heart rate and fitness), hackers may target these devices to steal health-related data. As healthcare becomes more digital, ensuring that personal and patient data remains secure will be even more challenging.

Key Takeaways:

- Personal and patient data can be stolen through methods like phishing, malware, and social engineering.
- Hospitals must protect sensitive data by implementing robust cybersecurity protocols and regularly training staff on data protection.

Lecture 3: The importance of passwords, MFA, and authentication

Think of your **password** as the key to your house. If someone else gets that key, they can enter and take whatever they want. In the digital world, a **password** is the first line of defense protecting your accounts and sensitive information. However, passwords alone are not always enough.

•**Multi-Factor Authentication (MFA)** is like adding a second lock to your door. Even if a hacker gets your key (password), they still need another form of authentication, like a fingerprint, a code sent to your phone, or even facial recognition.

•**Authentication** is the process of proving who you are. In a hospital setting, authentication ensures that only authorized personnel can access sensitive patient information.

Real-World Example:
In a hospital, nurses and doctors access patient records through a secure login process. A strong password and MFA are essential to ensure that only authorized medical staff can view sensitive patient information. Without these protections, an attacker who steals a password could easily access private data.

Future Example:

As hospitals implement more sophisticated technologies, such as biometrics or facial recognition systems, the authentication process will become even more secure. For example, an emergency room physician might use facial recognition to quickly access a patient's records in critical situations, ensuring that only authorized personnel can make decisions.

Key Takeaways:

- **Strong passwords** are crucial for protecting sensitive information.
- **Multi-Factor Authentication (MFA)** provides an additional layer of security.
- **Authentication** ensures that only authorized individuals can access sensitive data.

Multi Factor Authentication

Lecture 4: Why phishing works and how to spot it

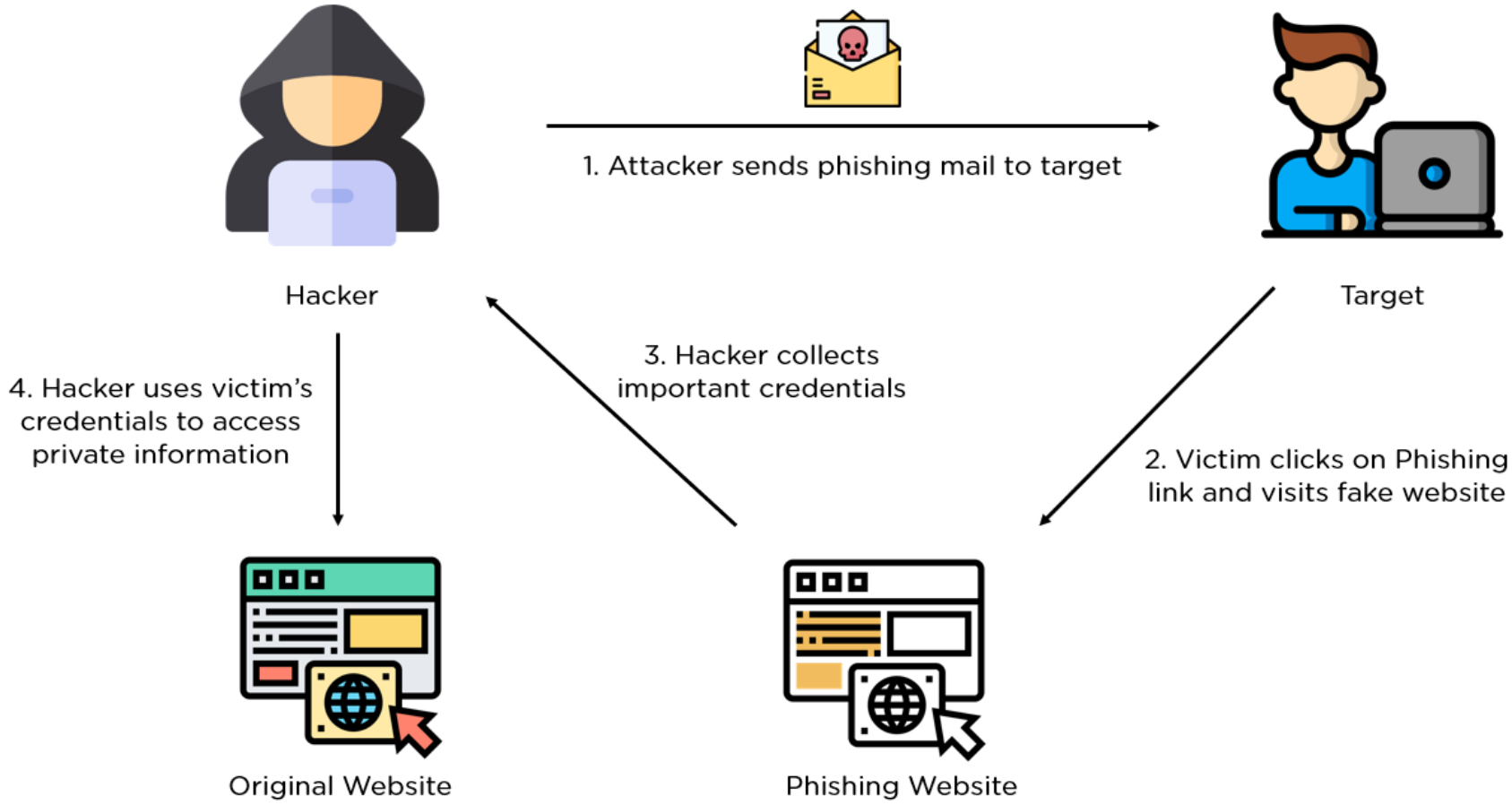
Introduction to Phishing:

Imagine someone knocks on your door and asks for your house key, pretending to be your neighbor. You think they're trustworthy, so you hand over the key, only to find out later that it was a burglar. In the digital world, **phishing** is when cybercriminals trick people into revealing sensitive information, such as passwords, credit card numbers, or patient data.

Phishing attacks typically occur via email or text message, but they can also happen on social media or through phone calls. The attacker will often impersonate a trusted entity, such as a hospital administrator, co-worker, or vendor.

How Phishing Works:

- **Fake Emails**: A hacker might send an email pretending to be from your boss, asking for sensitive information like your password or a link to click on.
- **Malicious Links or Attachments**: In many phishing attacks, the hacker will ask you to click on a link or open an attachment. If you do, malware can be installed, and your data can be stolen.



How to Spot Phishing:

1.Check the Sender's Address: Often, phishing emails come from addresses that look suspicious or unfamiliar.
2.Look for Typos: Phishing emails often contain spelling or grammatical errors.
3.Verify Requests: If you receive an email asking for sensitive information, verify it by contacting the person or organization directly.

Real Example:

In 2018, a phishing attack at a healthcare provider led to the compromise of over 30,000 patient records. The hacker used a fake email impersonating a hospital administrator and tricked an employee into providing their login credentials, leading to unauthorized access to sensitive data.

Lecture 5: Why phishing works and how to spot it

Rule of thumb:
When in doubt, **don't click — check it out.**

Why Phishing Works

Phishing works because it **tricks people emotionally and psychologically**.

- **Urgency:** Messages create panic ("Your account will be locked!") so you act without thinking.
- **Authority:** They pretend to be banks, government, or your boss - people you *trust*.
- **Curiosity or Greed:** "You won a prize!" or "Check out this invoice!" - people get tempted.
- **Lookalike Details:** Fake emails and websites *look* almost identical to real ones - logos, sender names, links making it hard to tell.

Humans, not systems, are the weakest link. Hackers know this and **exploit attention, trust, and emotion**.

Here are your super-easy phishing red flags:

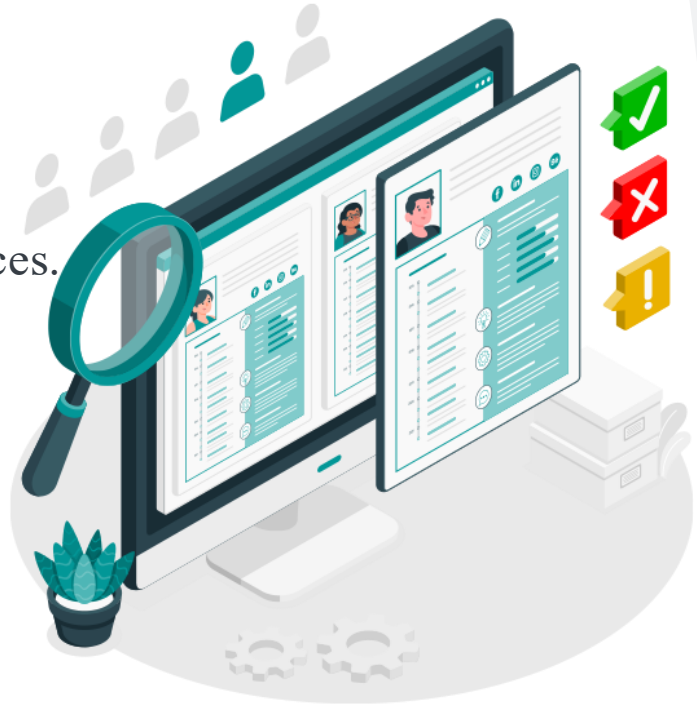
- Weird sender address: Like support@amaz0n-help.com instead of amazon.com.
- Grammar mistakes: Sloppy writing, weird phrases, odd greetings.
- Urgency or threats: "ACT NOW OR LOSE ACCESS!" — real companies rarely talk like that.
- Suspicious links: Hover (don't click!) and you might see a shady URL under a pretty button.
- Requests for sensitive info: Banks never ask for passwords or SSNs via email or text.
- Unusual attachments: Random attachments you weren't expecting are a huge red flag.

Future Example:

With AI becoming more advanced, phishing attacks may become even more convincing. AI could allow attackers to mimic the voice or writing style of a colleague or supervisor, making it even harder to distinguish between a real request and a malicious one.

Key Takeaways:

- Phishing attacks trick individuals into revealing sensitive information.
- Always verify emails or phone calls asking for personal data.
- Be cautious when clicking on links or opening attachments from unknown sources.

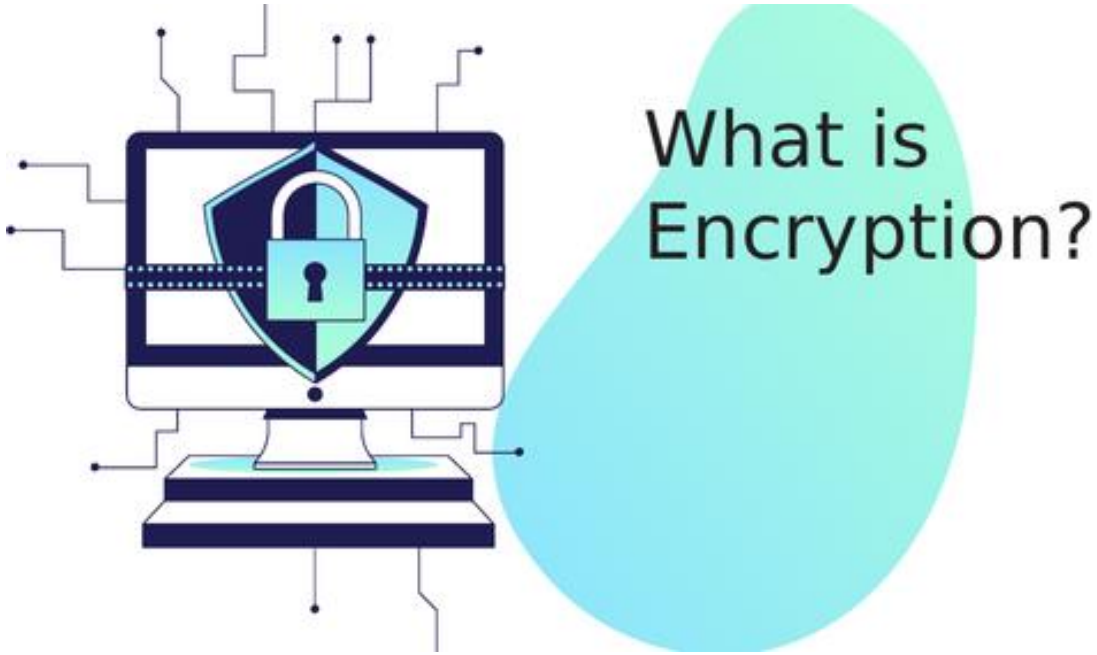


Lecture 6: The basic idea behind encryption

What is Encryption?

Imagine you're sending a very private letter through the mail - maybe a patient's health record. Would you trust just folding it and handing it to a random mailman? Probably not. Instead, you would lock it in a strong, unbreakable box, and only the person you're sending it to has the key to open that box.

In cybersecurity, **encryption is that locked box**. It protects sensitive information, like patient records, lab results, and billing details. so that even if someone intercepts it along the way, they can't read it. They just see a bunch of scrambled, meaningless letters and numbers.



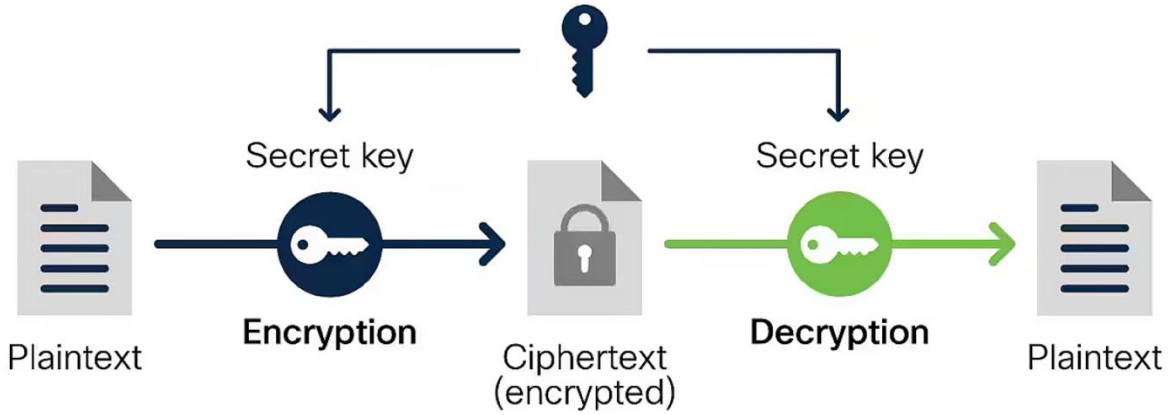
That's what encryption does:

It locks up important information so that only the right person can unlock and read it.
Even if someone else grabs it during delivery, all they would see is a locked box they can't open.
In the digital world, encryption scrambles information like patient records, lab results, or emails into a secret code. Only someone with the correct "key" can unlock and understand it.

Encryption is like putting your data in a locked box, with only the person with the key being able to open it. When information is **encrypted**, it's transformed into a code that can't be read unless you have the key to decrypt it. In the context of healthcare, encryption is essential for protecting patient data during transmission or when stored on servers.

How Encryption Works?

Encryption works by converting readable data (like patient names and medical records) into an unreadable format using a special algorithm. Only someone with the proper **decryption key** can turn it back into its original form.



Step 1: You take readable information (like a diagnosis) and scramble it into unreadable nonsense.

Step 2: You lock that scrambled message with a special digital "key."

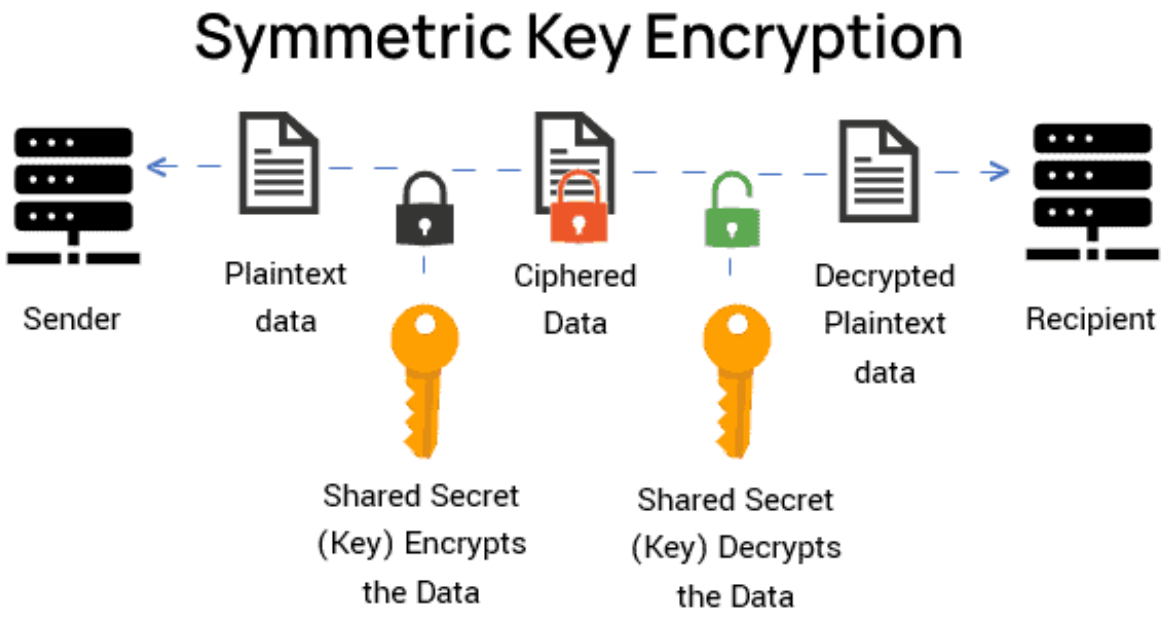
Step 3: Only the person with the matching key can unlock it and see the real information.

Scramble the Information:
The computer takes normal information (like “Patient John Doe, blood test normal”) and turns it into a random, unreadable mess like “7x@9!f#2z”.

Lock it with a Key:
A special digital “key” is used to scramble the information. Without this key, no one can understand what the message says.

Send it Safely:
Even if a hacker or thief grabs the scrambled information, they can’t do anything with it because it just looks like nonsense without the right key.

Unlock with the Key:
When the right person (like the patient or a doctor) gets the message, their system uses the matching key to unscramble the information and read it normally.



Lecture 7: The basic idea behind encryption

Encryption is like locking important patient information in a box that only trusted people can open.
It keeps our patients' privacy safe, even if bad actors are trying to break in.

Cybersecurity in the healthcare industry is of paramount importance. By understanding the core concepts of threats, vulnerabilities, data theft, authentication, phishing, and encryption, hospital staff can better protect patient data and maintain trust in the system. In a world where cyberattacks are becoming more sophisticated, education and vigilance are key to safeguarding sensitive information.

Why Encryption Matters in Hospitals

- **Protects Patient Privacy:** Keeps sensitive medical information safe from hackers and outsiders.
- **Builds Trust:** Patients trust hospitals to keep their personal information secure.
- **Meets Legal Requirements:** Laws like HIPAA require strong protection of patient data, and encryption is one of the best ways to do that.

Common Cybersecurity Threats to Watch Out For

- **Phishing Emails:** Fake emails that pretend to be from your boss, HR, or a hospital vendor. They might ask you to click a link or send personal information.
- **Weak Passwords:** Using simple passwords (like "12345" or "password") makes it easy for hackers to break into hospital systems.
- **Lost Devices:** A stolen laptop or phone without protection could expose hundreds of patient files.

Tips to Stay Safe

- **Be suspicious of urgent messages** asking you to click links or share information.
- **Use strong, unique passwords** for work systems — and change them regularly.
- **Lock your devices** when you step away, even for a minute.
- **Report anything suspicious** to your hospital's IT/security team immediately.

Real Example:

When a hospital transfers a patient's medical records to a specialist in another city, the data is encrypted before it's sent over the internet. Even if a hacker intercepts the data, they won't be able to read it without the decryption key.

Eg. Hospital Portal

- When a patient logs into the hospital's online portal to check lab results:
- The information is encrypted while it travels across the internet.
- Even if a hacker tries to intercept it, all they would see is scrambled code — not the real test results.
- Only the hospital system and the patient's account have the keys needed to "unscramble" and display the real information.

Future Example:

As healthcare systems adopt more cloud-based technologies, encryption will be crucial in protecting patient data stored on these platforms. For instance, patient records uploaded to a cloud server must be encrypted to prevent unauthorized access.

Key Takeaways:

- **Encryption** ensures that sensitive data remains unreadable to anyone without the proper key.
- It is essential for protecting patient data during storage and transmission.
- Healthcare providers must implement encryption in their systems to prevent unauthorized access to sensitive information.

STEVENS
INSTITUTE OF TECHNOLOGY
1870

THANK **YOU**

Stevens Institute of Technology
1 Castle Point Terrace, Hoboken, NJ 07030