eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Helping Healthcare Providers Adopt
Digital Health Technologies and Achieve
HIE Connectivity in the District

DCPCA
DISTRICT OF COLUMBIA
PRIMARY CARE ASSOCIATION

ARPA Home and Community Based Services (HCBS) Digital Health Technical Assistance (TA) Program

Security Awareness & Privacy

March 15, 2024

How to Engage

- Use **Chat** to share questions and comments with the group

- Use **Raise Hand** function to be queued up for commenting / unmuting and share your comments with the group

Learning Objectives

1. Provide basic, high-level, knowledge of the most common types of cyber security threats
2. Bring attention to habits and behaviors we all can employ to minimize the risk of cyberattacks and better protect the sensitive data contained within your EHR
3. Review HIPAA regulatory requirements, including the Privacy Rule, Security Rule, and Breach Notification Rule, to help protect the data contained within your EHR and maintain compliance with Federal mandates
4. Provide practical tools, tips and resources to help your organization build a culture of security

What is a cyber attack?

“A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device” - IBM

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

State of Cyberattacks

Chicago Children's Hospital Outage Continues After Cyberattack

Nearly a week after a cyberattack hit Lurie Children's Hospital in Chicago, email, phone, and electronic systems remain offline. The hospital proactively took its systems offline in the wake of...

Insurance Broker Data Breach Impacts 1.5M Individuals

January 31, 2024 - Insurance brokerage company Keenan & Associates recently notified more than 1.5 million individuals of a data breach. Keenan provides insurance and risk management solutions for schools, colleges, and healthcare organizations. According to a breach notice provided to the Maine Attorney General's Office, Keenan discovered disruptions on...

Healthcare Data Breaches Continue to Impact Patients in New Year

January 22, 2024 by Jill McKeon

In 2023, more than 540 organizations reported healthcare data breaches to HHS, impacting upwards of 112 million individuals. As the new year begins, the aftermath of 2023 breaches continues to...

North Kansas City Hospital Impacted By PJ&A Data Breach

January 08, 2024 by Jill McKeon

Missouri-based North Kansas City Hospital (NKCH) and its transc
recently notified more than 500,000 individuals of a third-party da

PJ&A Data Breach Fallout Continues, 4M Additional Individuals Impacted

January 30, 2024 by Jill McKeon

Concentra Health Services filed a data breach report with HHS in January tied to a previously reported breach at Perry Johnson & Associates (PJ&A), a medical transcription company....

Mississippi Health System Suffers Ransomware Attack, 253K Individuals Impacted

January 24, 2024 by Jill McKeon

Singing River Health System in Mississippi suffered a ransomware attack in August 2023 that r
breach. The breach impacted 252,890 individuals in total, according to a notice provided...

Kentucky Health System Confirms Ransomware Attack Impacting 2.5M Individuals

December 11, 2023 by Jill McKeon

Kentucky-based Norton Healthcare confirmed that a May 2023 ransomware attack on the heal
million individuals, according to a report filed with the Maine Attorney General's...

Source: https://healthitsecurity.com/topic/latest-health-data-breaches

Impact and Consequences of a Cyberattack

Direct Patient Care

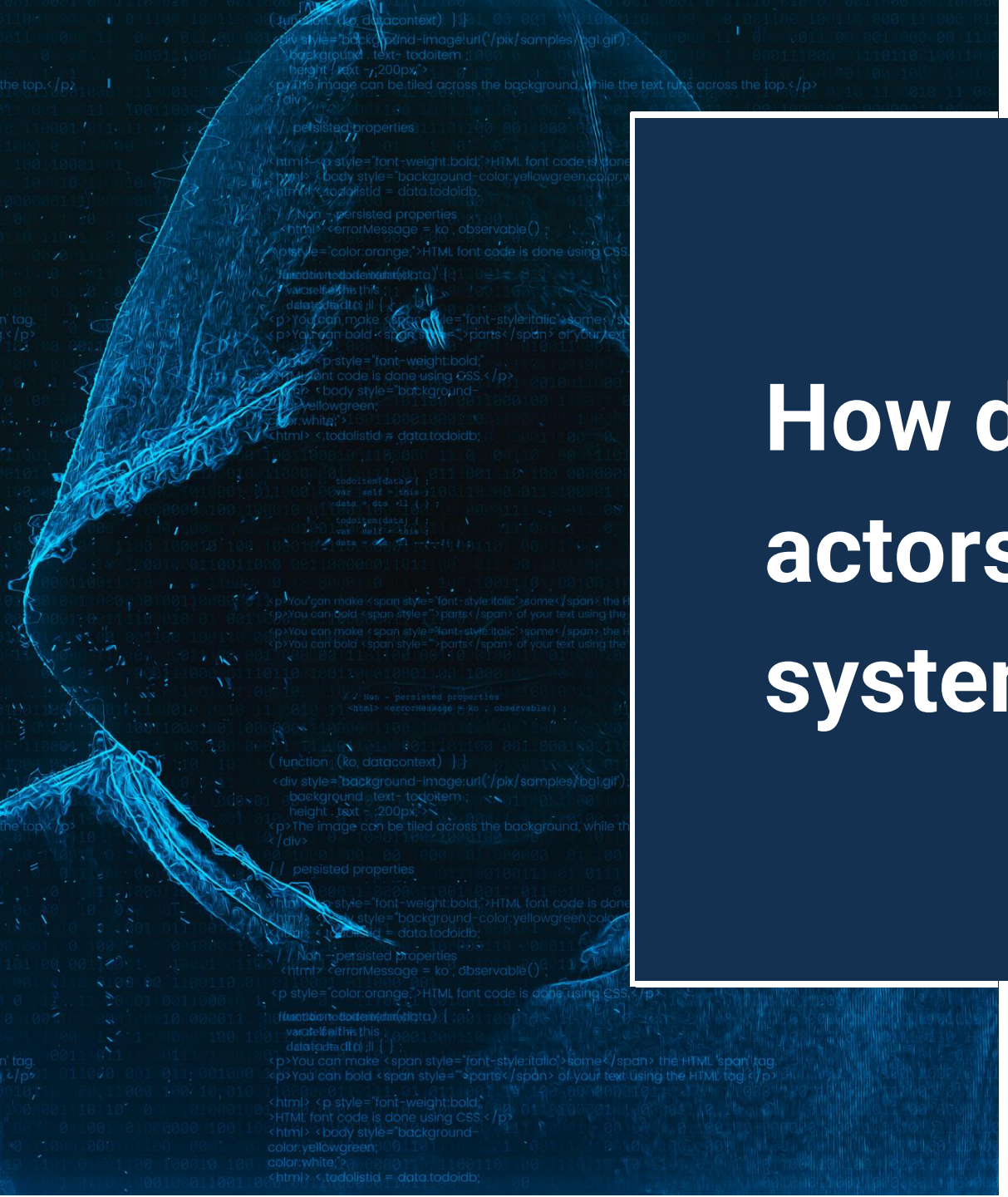
- Medical devices stop working or are corrupted
- Medical records including prescriptions, diagnoses, therapies become inaccessible or permanently lost
- Payment systems are down
- Forced to use to temporary paper system that can cause enormous time lags, inefficiencies, and errors

Practice

- Financial losses due to:
  - paid ransom
  - lawsuits
  - system recovery costs
  - regulatory penalties
- Damaged reputation
- Lost patient trust
- Strained employee morale/burnout

Patients & Employees

- Identity Theft: Malicious actors can use your Name, Address, Social Security and Date of birth to open new accounts and take money out of your bank account
- Identity theft and fraud don't only affect individuals, but their family, friends and coworkers



How do malicious actors break into your systems?

eHealthDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Social Engineering

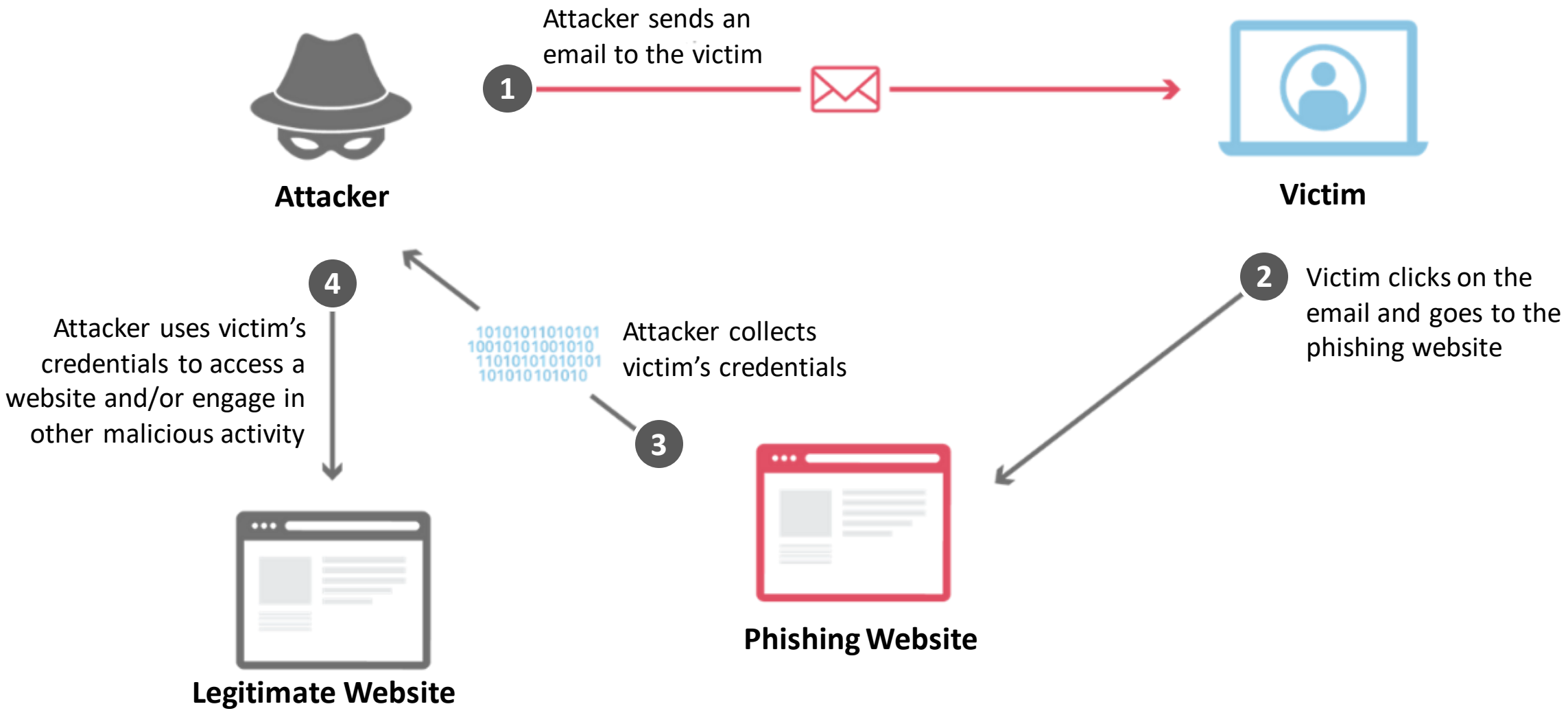
Use of deception to manipulate well-meaning individuals into divulging confidential information or that person's personal information which may be used for fraudulent purposes.

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.

Anatomy of Cyber Attack



Why Are Phishing Attacks Common?

- **Effective**: Phishing attacks are often successful because they exploit human vulnerabilities rather than technical ones.
- **Low Cost**: Phishing attacks can be launched at minimal cost and effort, making them accessible to a wide range of attackers, including those with limited technical expertise.
- **Easy, Yet Sophisticated**: Phishing attacks have become more sophisticated, difficult to detect, and easier to create with tools like Artificial Intelligence (AI).

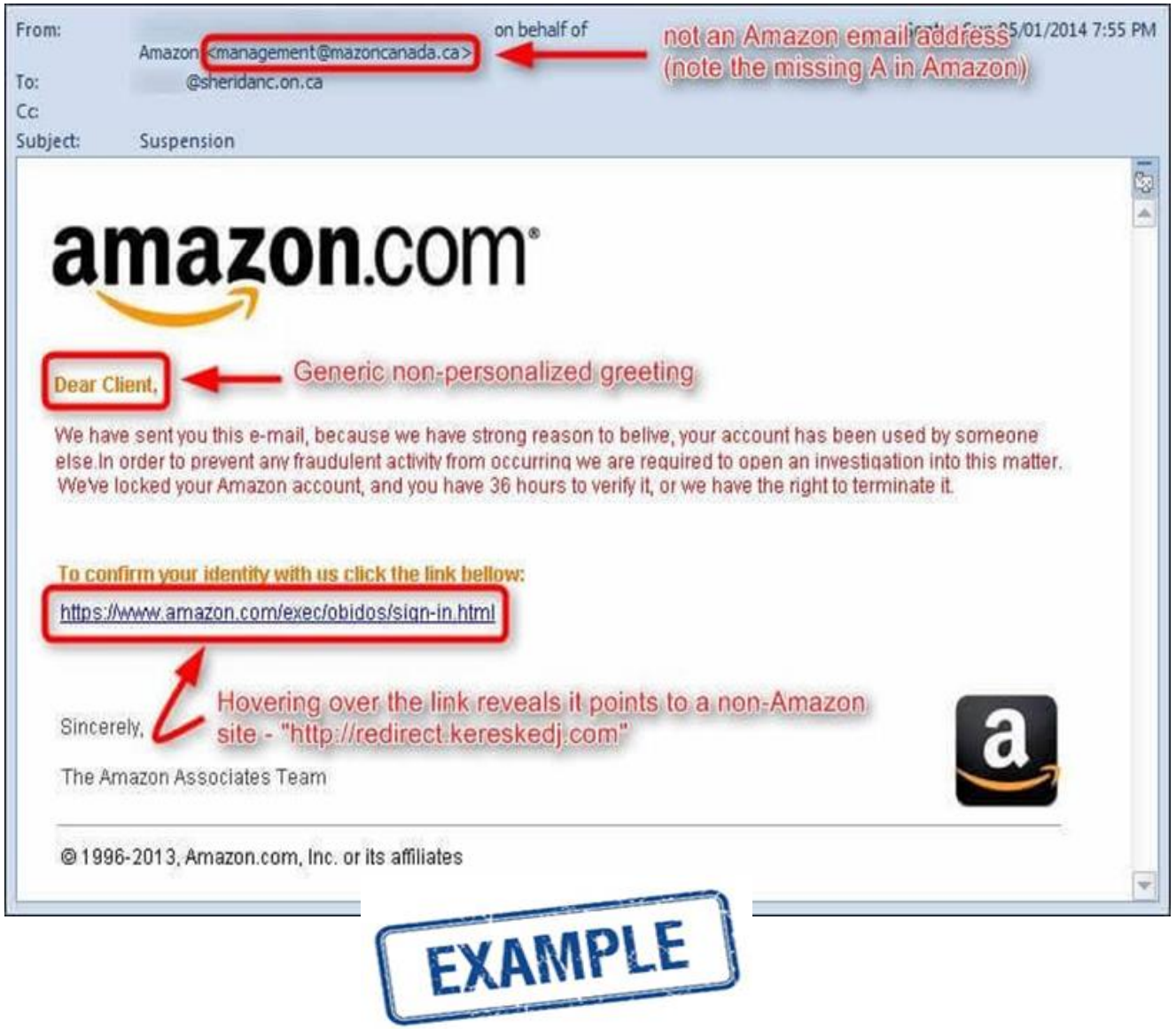
Phishing Attacks can be conducted using multiple attack channels:

Email

Phone Call(Vishing)

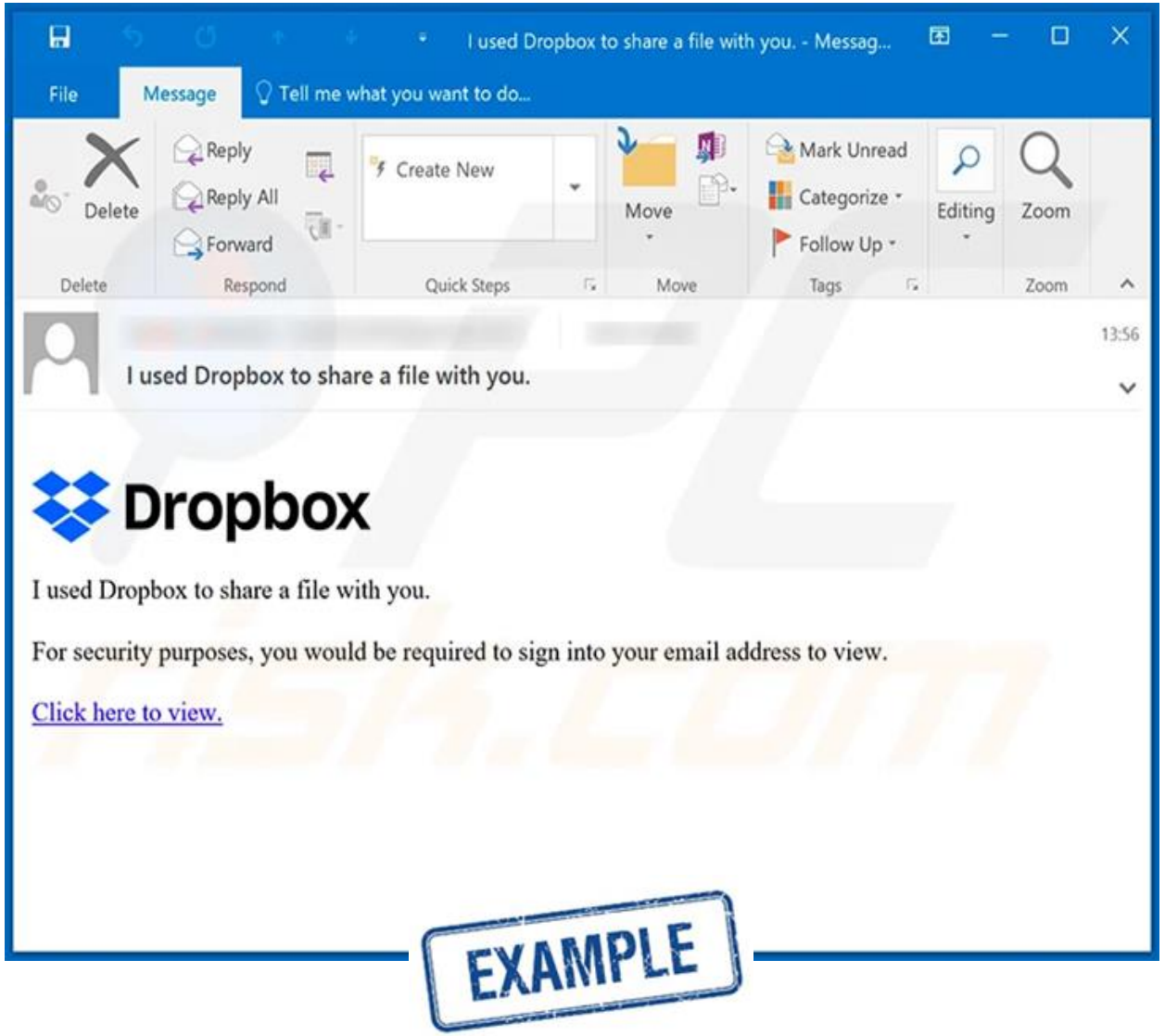
Texting (SMiShing)

Phishing Example: Suspicious Links



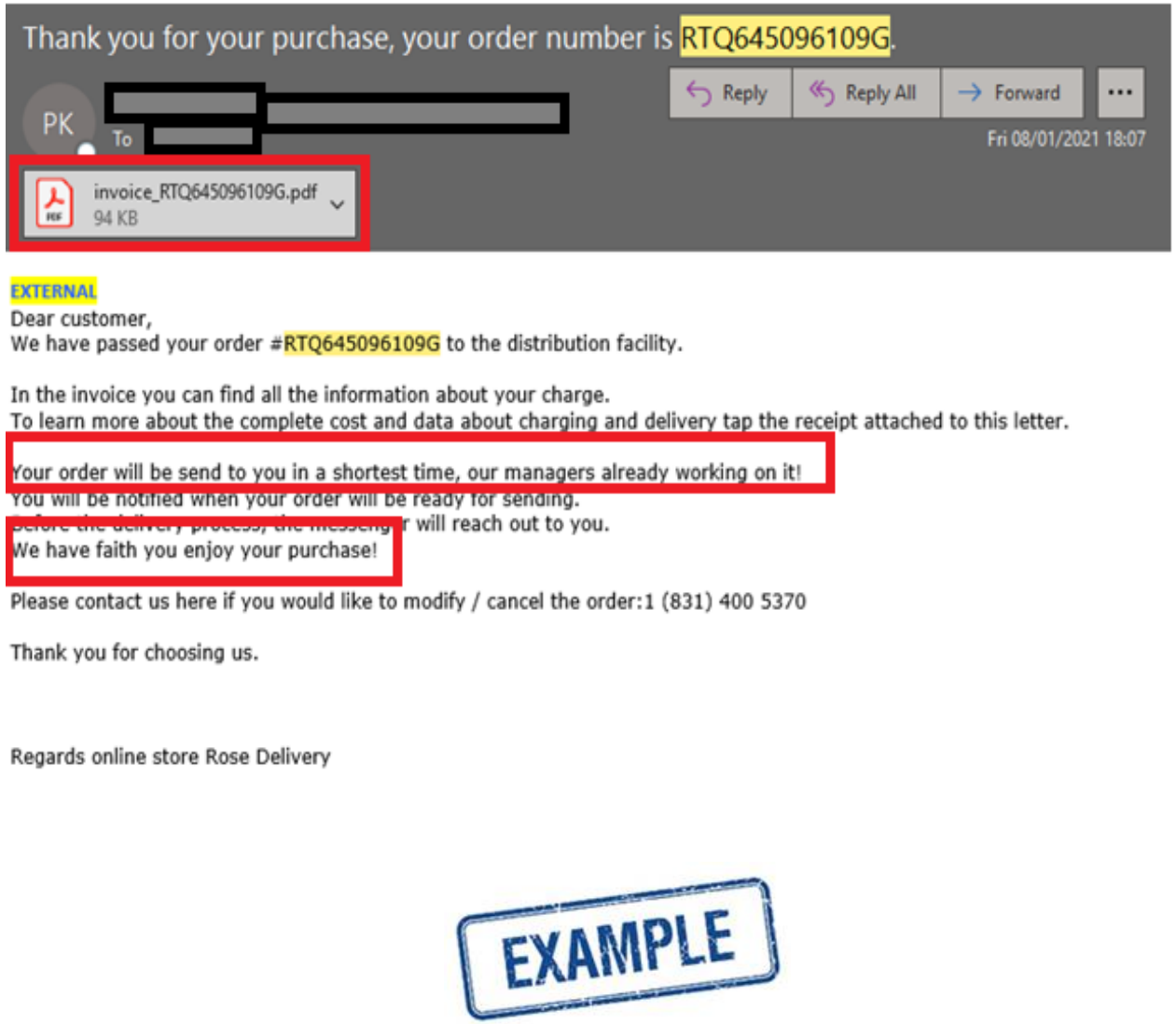
- Appears to be from well-known Company like Amazon asking you to sign-in and **urgently** correct an issue with your account
- **Links** points to a website pretending to be from the company's legitimate site and asks to log in
- *TIP: **DO NOT CLICK** on any links in the email – If in doubt, directly log-in to your account by typing the company address directly into your web browser.*

Phishing Example: Cloud File Sharing



- Contains a **link** to what appears to be a shared file on OneDrive, Google Docs, Dropbox or any other file sharing site
- Link points to a website pretending to be from a file sharing site and requests you to log in
- *TIP: **DO NOT CLICK** any links in the email instead login to your account and find the file shared by name – Remember to verify sender's identity*

Phishing Example: Fake Invoice



Thank you for your purchase, your order number is RTQ645096109G.

Reply | Reply All | Forward | ...

PK [redacted]

To [redacted]

Fri 08/01/2021 18:07

invoice_RTQ645096109G.pdf
94 KB

EXTERNAL

Dear customer,
We have passed your order #RTQ645096109G to the distribution facility.

In the invoice you can find all the information about your charge.
To learn more about the complete cost and data about charging and delivery tap the receipt attached to this letter.

Your order will be send to you in a shortest time, our managers already working on it!
You will be notified when your order will be ready for sending.
Before the delivery process, the messenger will reach out to you.
We have faith you enjoy your purchase!

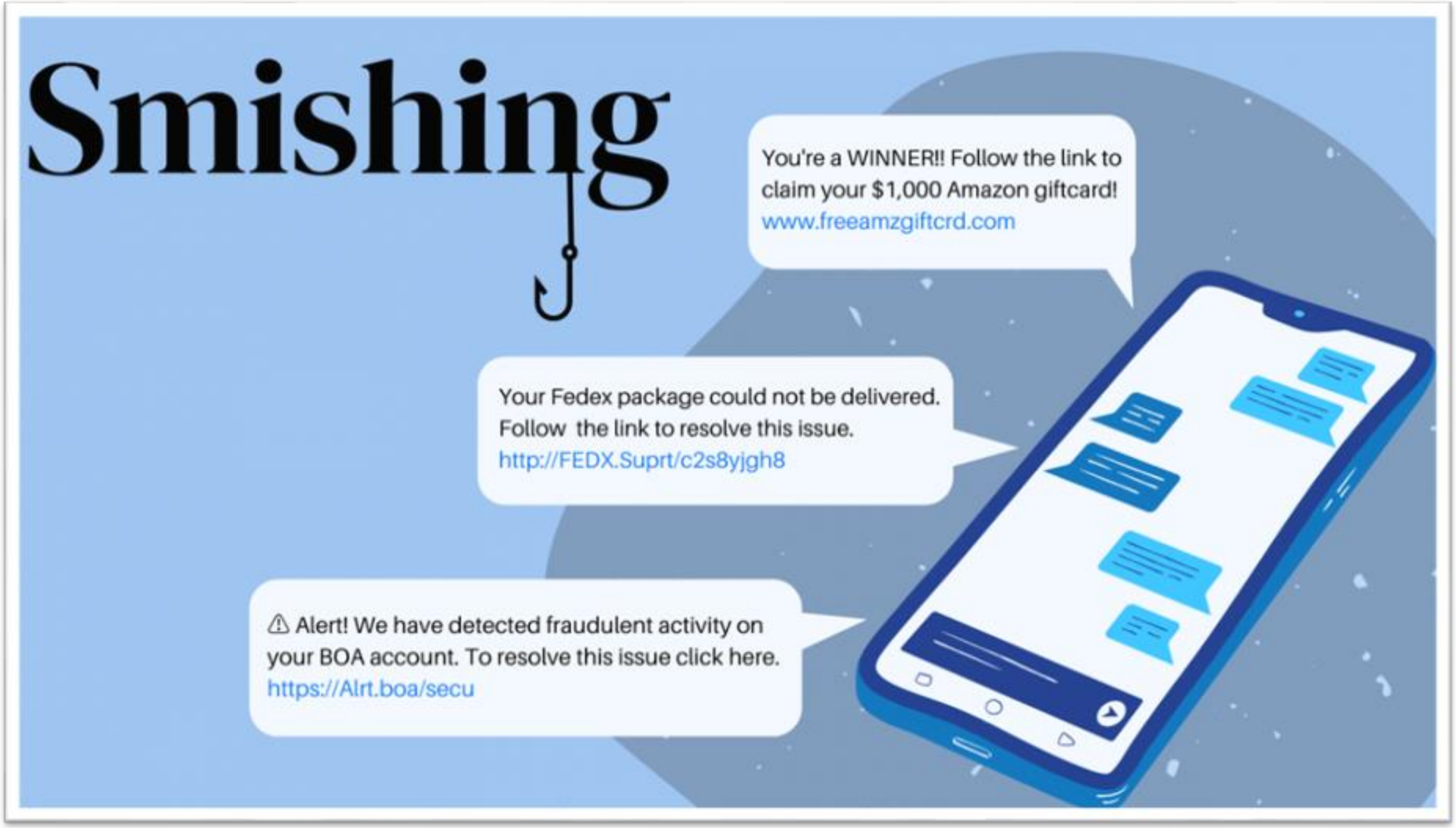
Please contact us here if you would like to modify / cancel the order:1 (831) 400 5370

Thank you for choosing us.

Regards online store Rose Delivery

- Contains an **attachment** presented as an unpaid invoice and claims service will be terminated if invoice is not paid in full
- Targets individuals (by pretending to be a retailer) or business (by impersonating a vendor or a supplier)
- *TIP: **DO NOT DOWNLOAD THE ATTACHMENT**. Contact the vendor/service directly using official contact information before submitting payment*

SMiShing


Smishing
You're a WINNER!! Follow the link to claim your $1,000 Amazon giftcard!
www.freeamzgiftcrd.com
Your Fedex package could not be delivered. Follow the link to resolve this issue.
http://FEDX.Suprt/c2s8yjgh8
⚠ Alert! We have detected fraudulent activity on your BOA account. To resolve this issue click here.
https://Alrt.boa/secu

PHISHING RED FLAGS

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common red flags in phishing include:

1. Urgent or threatening language
2. Suspicious sender information
3. Out of the ordinary requests
4. Impersonal or generic greetings
5. Requests for personal information
6. Misspellings or grammatical errors
7. Unnecessary attachments or attachments end in ".exe"

Which of the seven red flags do you think is the hardest to detect? What makes you say that?

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Can you identify the signs of a phishing email?

From: Helpdesk <helpdesk-infotech@gmail.com>

To:

Subject: Fraud Alert!

Attachment: Password Reset Details.exe

Dear Info-Tech user,

We have recently detected a login to your online account that was not performed by you. In order to rectify this situation please go to InfoTech website here to change your password to ensure your account is secure. The documnt attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details and I will verify your account for you. If you fail to do so by next week will result in your acount being deleted.

Sincerely,

Info Tech

Identifying a phishing email

From: Helpdesk <helpdesk-infotech@gmail.com> 1

To:

Subject: Fraud Alert! 2

Attachment: Password Reset Details.exe 3

Dear Info-Tech user, 4

We have recently detected a login 5 our online account that was not 6 rmed by you. In order to rectify this situation please go to InfoTech website here to change your password to ensure your account is secure. The 7 document attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details 8 will verify your account for you. If you fail to d 9 by next week will result in your acount being deleted.

10

Sincerely,

Info Tech 11

EXAMPLE

RECOGNIZE & REPORT PHISHING

Practical tools and tips to avoid getting phished

Be cautious with links, attachments, and forms
Avoid clicking on suspicious links, opening attachments, or filling out forms in emails

Verify links before clicking
Hover over links to ensure they lead where they claim. Check for "https" in the URL, correct spelling, and legitimacy of the website

Keep software updated
Maintain up-to-date web browsers and use anti-phishing plug-ins or add-ons for extra security

Do not give out personal information
Avoid providing personal information via email

Confirm requests directly
Reach out to the sender via a known, trusted method to confirm the legitimacy of the email

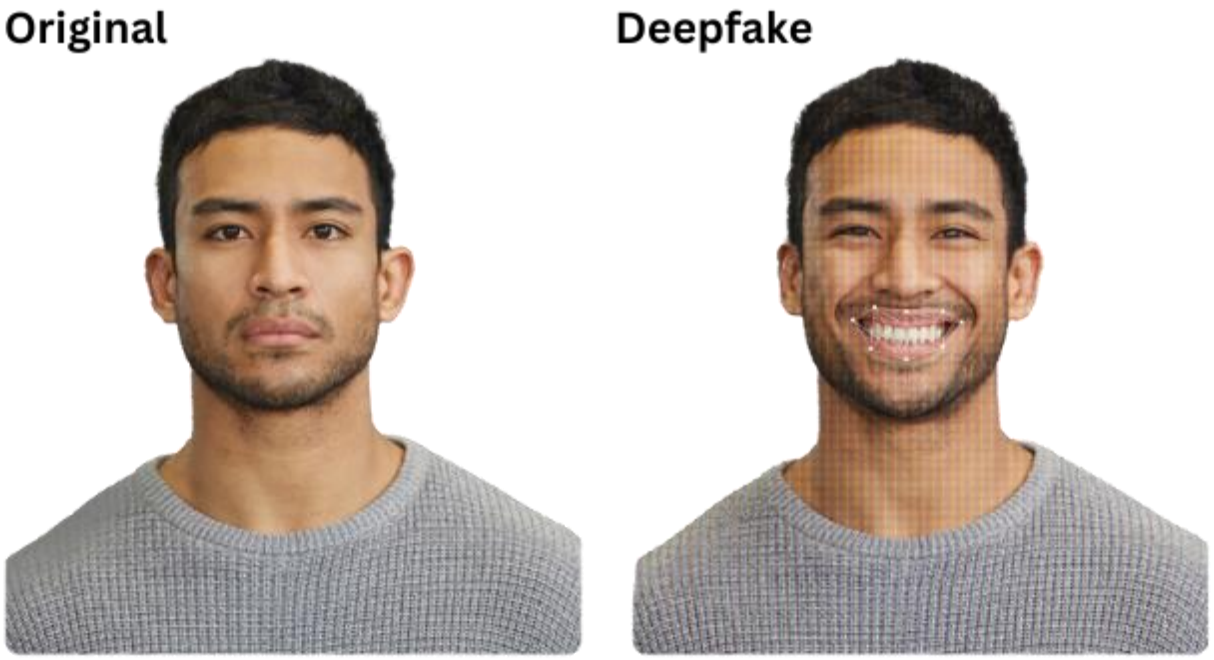
Contact IT for verification
If uncertain, contact your IT department or person to verify that the email is legitimate

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Social Engineering Trends

With Artificial Intelligence (AI), attackers can now create a digital twin of your face and voice and use them to say and do anything they want.

Three seconds of your Youtube, Facebook or Tiktok video is sufficient for an AI tool to clone your voice or your face.



PROTECT YOURSELF AGAINST SOCIAL ENGINEERING

- Don't perform any financial transactions, share passwords or personal information over the phone even if the voice sounds familiar.
- Never provide any confidential information when a representative unexpectedly calls you by phone. Ask to hang up and call back using a known number to verify the caller is legitimate.
- If the caller insists that you stay on the call, this is a red flag. Hang up immediately and alert your IT/security department.
- Minimize the amount of personal data on social media platforms. We often share our personal information indirectly on social media. However, malicious actors can can use this information to conduct Brute Force attacks.

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Protecting Your Passwords

According to Department of Health and Human Services (HHS) 85% of cyber criminals accessed critical systems and data using stolen credentials

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

PASSWORD TIPS & BEST PRACTICES

Convert a phrase or sentence to a strong password

Choose a phrase you can remember and reduce it to the first letters of each word, adding some numbers, capitalization, and punctuation

Examples:

My jersey number when I played competitive soccer was 27! → Mj#wlpcsw27!

"For the first time in forever" - Disney's Frozen → 4da1stTymein4eva-Frozen

Change default passwords

Avoid reusing the same password across multiple accounts

Use a password manager

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Two of the following passwords are considered strong passwords.
Which two are they?

a) **ilovecats**

b) **14A&A41**

c) **iloveKatzs123**

d) **!cedTisgr84$umm3R**

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Two of the following passwords are considered strong passwords.
Which two are they?

a) ilovecats

b) 14A&A41

c) iloveKatzs123

d) !cedTisgr84$umm3R

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

How To Protect Your Practice From Cyber Threats?

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

HIPAA Overview

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

Good Security best practices begin with HIPAA.

What is HIPAA compliance ?

HIPAA compliance is adherence to the physical, administrative, and technical safeguards outlined in HIPAA, which covered entities and business associates must uphold to protect the integrity of Protected Health Information (PHI).

Primary Purpose of HIPAA Regulations

The main objective of HIPAA regulations is to uphold and protect the data integrity of Protected Health Information (PHI). It includes three rules: Privacy Rule, Security Rule, and Breach Notification Rule

HIPAA Privacy Rule

creates standards for the privacy of PHI.

HIPAA Security Rule

standardizes the handling of electronically protected health information (ePHI)

Breach Notification Rule

mandates that covered entities and business associates must alert any affected parties whenever their protected health information is compromised

HIPAA PRIVACY RULE

Creates standards for the privacy of PHI

HIPAA Privacy Rule

- HIPAA applies to **"Covered Entities,"** defined by the Privacy Rule as a:
  - Health care provider that conducts certain transactions in electronic form
  - Health care clearinghouse
  - Health plan
  - Business associate (person or organization performing a function on behalf of a covered entity for which access to protected health information is needed

- Privacy is important because it:
  - Fosters trust between individuals/clients/patients and your organization
  - Protects PHI from loss, theft, and/or misuse

HIPAA Privacy Rule: Safeguard Requirements

- **Use and Disclosure** – A covered entity may not use or disclose PHI, except either:

  (1) as the Privacy Rule permits or requires

  (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

- **Get authorization** – get permission from the patient to use redacted ePHI for research, fundraising, or marketing.
- **Notice of Privacy Practices (NPP)** – An NPP is required to officially inform patients and subscribers of data-sharing policies.

CRISP DC Notice of Privacy Practices

Suggested Update to Notice of Privacy Practices

We have chosen to participate in the Chesapeake Regional Information System for our Patients ("CRISP"), a regional health information exchange ("HIE") serving the District of Columbia. CRISP is also affiliated with and shares data with other HIEs, including those in Alaska, Connecticut, Maryland, and West Virginia. As permitted by law, your health information will be shared with this exchange in order to provide faster access, better coordination of care and assist providers and public health officials in making more informed decisions. You may "opt-out" and disable access to your health information available through CRISP by calling 1-877-952-7477 or completing and submitting an Opt-Out form to CRISP by mail, fax or through their website at www.crispdc.org.

Suggested Update to NPP Acknowledgement Page

We participate in the CRISP health information exchange ("HIE") to share your medical records with your other health care providers and for other limited reasons. You have rights to limit how your medical information is shared. We encourage you to read our Notice of Privacy Practices and find more information about CRISP medical record sharing policies at www.crispdc.org.

Let's Discuss!

Can you email patients? If so, what policies does your organization have in place when communicating with patients via email?

Communicating with Patients via Email

Can you email patients?

- The HIPAA Privacy Rule allows covered health care providers to communicate via email provided there are safeguards in place:
  - HIPAA Standard 164.312(d) requires providers to implement procedures to verify that persons or entities seeking access to ePHI are who they claim to be
  - HIPAA Standard 164.306(b) requires providers to implement reasonable and appropriate security measures

Should you email patients? It depends….

- Some organizations explicitly consent patients to acknowledge or opt out of email communications
- EHR patient portals offer secure messaging communications
- Regular emails are not encrypted and is not secure, sometimes households share email addresses
- If a patient emails you first, you can assume that email is acceptable
- Share only appropriate information via email

HIPAA SECURITY RULE

Standardizes the handling of electronically protected health information (ePHI)

HIPAA Security Rule

- The HIPAA Security Rule outlines the requirements for the protection of electronic patient health information. The Security Rule refers to "Security Standards for the Protection of Electronic Protected Health Information."

HIPAA Security Rule: Administrative Safeguards

- **Risk management** – Risk assessment is an ongoing process that must be reassessed at regular intervals with measures put in place to reduce the risks to an appropriate level. A sanctions policy must be introduced for employees who fail to comply with HIPAA regulations.
- **Comprehensive Policies and Procedures** – Develop and consistently update a set of cybersecurity policies and procedures that align with industry best practices and comply with relevant regulations. These documents serve as a foundation for ensuring a consistent and secure approach to information security.
- **Train your staff** – You need to train employees on all ePHI access protocols and how to recognize potential cybersecurity risks such as phishing, hacking, and deception. A record of these sessions must be kept.
- **Incident Response Readiness** – Develop robust incident response plan in place, detailing the procedures to be followed in the event of a security incident. Regular drills and simulations are conducted to test the effectiveness of our response mechanisms.
- **Build contingencies** – You must be able to achieve ongoing business continuity, responding to disasters with a preparation process that keeps data safe.

HIPAA Security Rule: Technical Safeguards

- **Network encryption** – Encrypt any ePHI to meet NIST cryptographic standards any time it is transmitted over an external network.
- **Encrypt devices** – All end-point devices that access the system should be able to encrypt and decrypt data, this is particularly important for mobile and laptop devices.
- **Authenticate ePHI** – You must identify and authenticate ePHI and protect it from corruption, unauthorized changes, and accidental destruction.
- **Control access** – Each user is assigned a centrally-controlled unique username and PIN code to access the systems. Procedures must also be in place to govern when to release or disclose ePHI during an emergency.
- **Control activity audits** – Detailed logging is needed to track all ePHI access attempts and to monitor how ePHI data is manipulated.
- **Enable automatic logoff** – Users must be logged out after a certain set time frame, usually between 30 seconds and 3 minutes depending on the application or system.

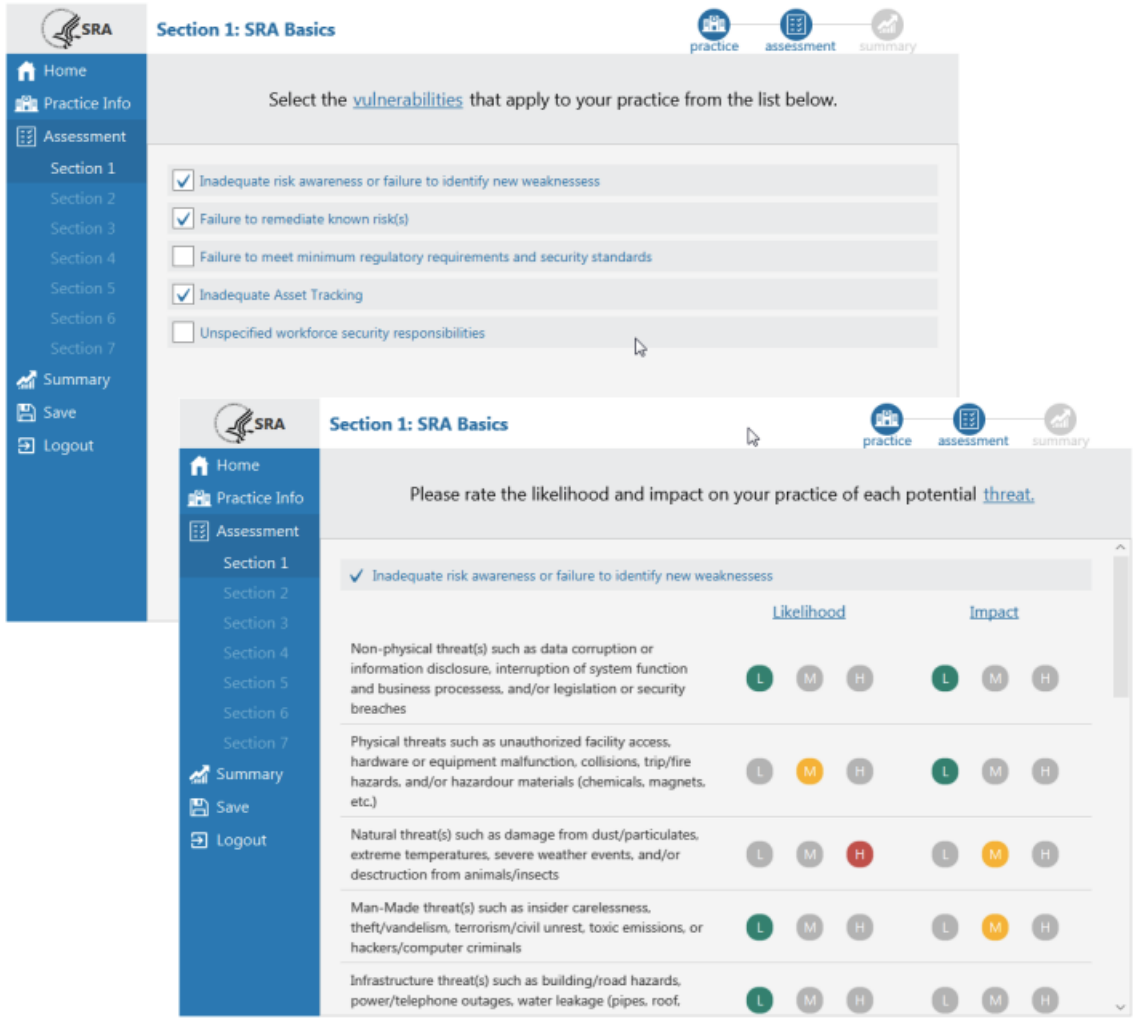
HIPAA Security Rule: Physical Safeguards

- **Control facility access** – You want to carefully track the specific individuals who have physical access to data storage – not just engineers, but also repair people and even custodians. You must also take reasonable steps to block unauthorized entry.
- **Manage workstations** – Write a policy that limits which workstations can access health data, describe how a screen should be guarded against parties at a distance, and specify appropriate workstation use.
- **Protect mobile devices** – You want a mobile device policy that removes data before a device is circulated to another user.
- **Track servers** – You want all your infrastructure in an inventory, along with information pertaining to where it's located. Copy all data completely before you move servers.

ONC: Security Risk Assessment Tool

- According to HIPAA §164.308(a)(1)(ii)(A), a covered entity or business associate must: " Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the organization"

- The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable, wizard-based Security Risk Assessment (SRA) Tool to aid in the identification and assessment of risks to ePHI
  - The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.



True or False?

My security risk assessment only needs to look at my EHR.

False! Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data.

True or False?

I have to outsource the security risk analysis assessment.

False! It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.

Security Risk Assessment Outcomes

Organizations should use information from their security risk assessment to understand and identify security and compliance gaps within their organization and implement appropriate strategies to rectify those gaps

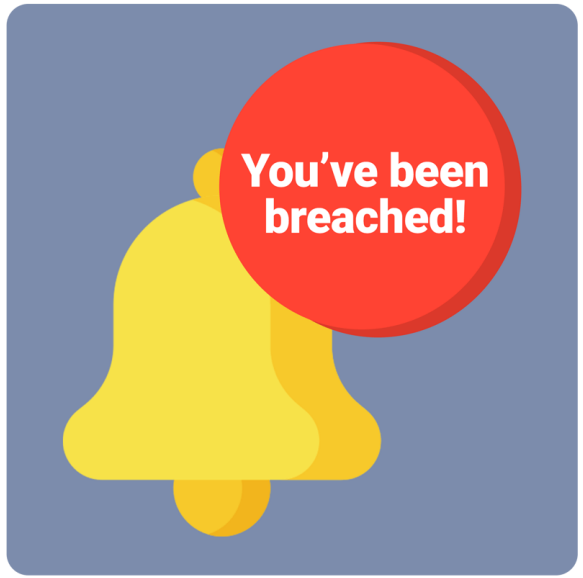
Breach Notification Rule

Sets requirements for who to notify in the event of a protected health data breach

HIPAA Breach Notification Rule

- **Know the notification process** – If a breach of ePHI occurs, you must make your patients aware and submit a Notice of Breach to the Secretary of HHS by completing the appropriate Breach of Unsecured Protected Health Information form.
  - If more than 500 records are involved, you also must also notify the media.
  - All of the immediate notifications must be completed within 60 days after discovery of the breach

- **Check twice for four** – Make sure that your breach notification message contains these four elements:
  - A description of the ePHI and personal identifiers involved in the breach
  - Who gained unauthorized access to PHI or related information
  - Whether details were simply seen or taken – viewing vs. acquirement
  - The degree to which risk mitigation has succeeded



What to do to minimize the impact of a breach?

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

3 PHASES OF BACKUP AND RECOVERY

Backup and recovery plans help to maintain compliance with HIPAA standards and minimizes the impact of a data breach if one occurs

1 **Assess**

2 **Implement**

3 **Review**

- Take a careful look at your data. This includes practice management (scheduling, billing etc.) and all electronic health records.
- Key Questions:
  - Where is your data kept?
  - How much of your data is stored there?
  - How much do you expect your data to grow in the next 4-5 years?
  - Who would be impacted? Think about what you can afford to lose.
  - How long can you afford to not have access to your data?

- Create backup policy and procedures. Most likely you'll want to do a weekly full back up with nightly differential backups. Depending on how often your data changes you may want to back up more frequently. For most practices nightly backups will be sufficient. All backups should be encrypted and stored securely.
- All practices must have the following key plans in place:
  - **Incidence Response Plan**
  - **Disaster Recovery Plan** (including business impact analysis, and backup/recovery plan)
  - **Business Continuity Plan** (ensures critical business functions continue during a disruption)
  - **Contingency Plan** (plan for alternative key systems)

1 **Assess**

2 **Implement**

3 **Review**

- Periodically verify your backup. Choose a couple of files you've backed up previously and restore them to see if the files are intact. This should be performed at least quarterly.
- Revisit your policies and procedures once a year.
- Key Questions:
  - Are your polices and procedures still appropriate for your practice.
  - What changes should you make to existing policies and procedures, if any?

Questions for your EHR vendor

If your EHR is hosted by an off-site vendor, often referred to as Software as a Service (SaaS) or an Application Service Provider (ASP) be sure to ask the following questions:

1. Do they have a backup plan that you can see? Can you have a copy?
2. What is their backup method?
3. What is their guaranteed recovery time? (How fast can they restore your data in the event of a disaster?)
4. How frequent are backups performed?
5. What is their guaranteed recovery point? (What's the most data you can lose in a disaster?)
6. What is the recovery process? (Do you manage it yourself through the web? Do you call a help desk or technician? Do you submit a ticket?)
7. How does your Service Level Agreement (SLA) address and guarantee the answers to the above questions?
8. What is the restitution process if they don't meet their guarantees?

Any reputable vendor should be able to provide you with this information. If they can't or won't then you should consider another vendor. Remember: You have a right to audit your vendor annually!

Your Cybersecurity Toolkit

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Your Cybersecurity Toolkit

- HHS Cybersecurity Awareness Training (CSAT)
- Contingency Planning Safety Assurance Factors for EHR Resilience (SAFER) Guide (recommended safety practices associated with planned or unplanned EHR unavailability)
- NIST Cryptographic Standards and Guidelines
- HHS Information on Submitting a Notice of a Breach
- ONC Cybersecurity Checklist Series
  - ONC Anti-Virus Checklist
  - ONC Backup and Recovery Checklist
  - ONC Access Control Checklist
  - ONC Maintenance Checklist
  - ONC Physical Access Checklist
  - ONC Network Access Checklist
  - ONC Password Checklist
  - ONC Mobile Device Checklist

Your Cybersecurity Toolkit

- Security Risk Assessment Resources
  - ONC Security Risk Assessment Tool (free SRA tool for small and medium sized businesses)
  - Posture (Commercial SRA tool and cybersecurity advisory services)
    - Full HIPAA Compliance Management
    - Expert Compliance Advise
    - HIPAA Policies and Procedures Templates

- Password Managers
  - Keeper Security
  - Bitwarden
  - 1Password

Your Cybersecurity Toolkit

- Policy Templates *(MS Word documents will be attached to follow-up email)*
  - Access Control Policy
  - Breach Notification Policy
  - Business Associate Policy
  - Computer Acceptable Use Policy
  - Cybersecurity Policy
  - HIPPAA Privacy – PHI Policy
  - Incident Response Policy
  - Password Policy
  - PHI Protection Policy
  - Physical Security Policy
  - Workforce Security Policy
  - Workforce Training Policy

Questions?

Upcoming eHealthDC Trainings

Training	Date	Training Type
Best Practices for Improving EHR Data Quality	Friday, March 22, 2024	EHR
Best Practices for Improving EHR Data Quality	Friday, March 26, 2024	EHR
eHealth DC Learning Community	Thursday, March 28 , 2024	EHR

Training	Date	Training Type
Pop/Health/Analytics	Tuesday, March 19, 2024	HIE
Social Needs Screening Tool	Wednesday, March 27, 2024	HIE