

Security Overview

Joseph Balberde

North Country Community Mental Health
Information Technology Director

2-5-2019

Protected Health Information

Individually Identifiable Health Information (IIHI): is information that relates to the individual's past, present, or future physical or mental health condition, provision of healthcare, or payment for healthcare, and that identifies or could reasonably be used to identify the individual.

Protected health information (PHI) under US Federal Law is “individually identifiable health information” held or transmitted by a covered entity (NCCMH) or its business associate (provider), in any form or media, whether electronic, paper or oral.

Identifiers:

- Name: First/Last or Alias of recipient or relatives, employers or household members
- Address: smaller than state: street address, city, county, zip code (or equivalent).
- Dates: dates that are directly related to an individual including birth date, admission date, discharge date, and death date.
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers: serial numbers, including license plate numbers
- Device identifiers: serial numbers (prosthetics, hearing aids, individual's serialized property)
- Web URLs
- Internet Protocol (IP) addresses
- Biometric identifiers: finger and voice prints
- Photographs: full face and any comparable images
- Any other unique identifying number, characteristic, or code

Minimum Necessary Rule

01

Disclose only
information necessary
for coordination of care

02

Disclose only to people
necessary for
coordination of care



Email

Email

- ▶ Transmission
 - ▶ Emails must be encrypted to be considered secure
- ▶ Authentication
 - ▶ Usernames and passwords are generally considered proof of authentication

When sending emails include only
Client number
First and Last initials

This is all that is necessary to identify a client
The first and last initial are included to verify the client



All emails must be encrypted even if they only contain
the client number and initials



Voice Communication

Phone Calls

- ▶ Transmission
 - ▶ Phone calls are generally considered secure in their transmission
- ▶ Authentication
 - ▶ In most cases voice and or phone number is enough to verify the recipient



Texting

Texting

- ▶ Transmission
 - ▶ Text messages are often not encrypted and not considered secure in transmission
- ▶ Authentication
 - ▶ Text messages often do not require a username and password and are not considered to be authenticated

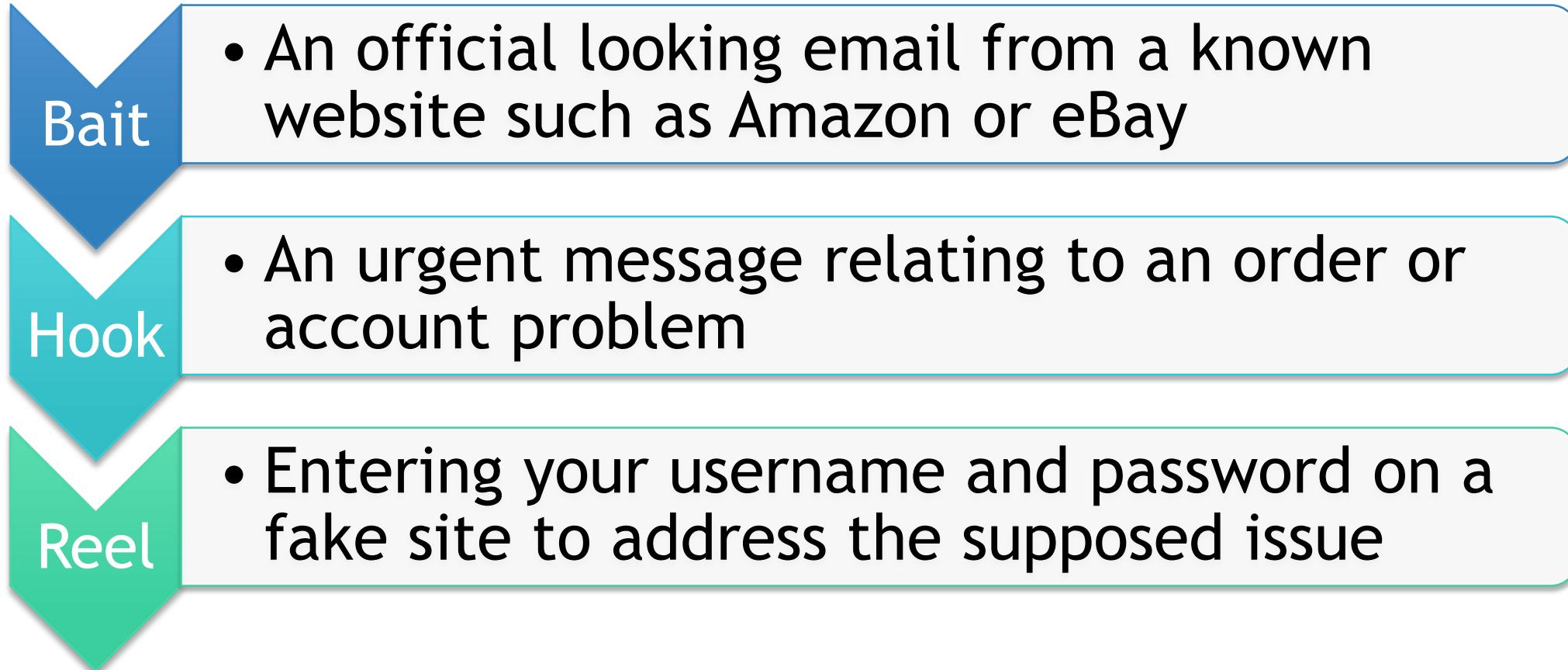


Texts are NOT secure



Email Phishing and Spoofing

Email Phishing



Email Spoofing

Creating a forged email

This is generally done by sending out an email with a fake email header.

Creating an email account with your display name

This can be done by creating an account with your display name using a free email service.

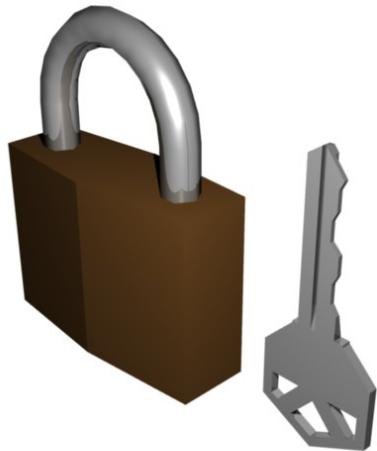
How can you protect yourself?

Question

Does the email request make sense from the recipient?
Is there broken sentence fragments or poor English?

Look

Pay close attention to the email address; does it have
@norcocmh.org or match the expected address?



Multi-Factor Authentication

Multi-Factor Authentication (MFA)

- ▶ Some times called two-factor authentication
- ▶ Similar to how your bank may text or email you when you sign in from a new computer or location
- ▶ NorthStar will require MFA
- ▶ MFA applications are available on the Google play/Apple App Store



Questions?

Joseph Balberde

jbalberde@norcocmh.org

231-439-1294