DATA SECURITY

ANNUAL EMPLOYEE TRAINING

NEW YORK STATE MIGRANT EDUCATION PROGRAM

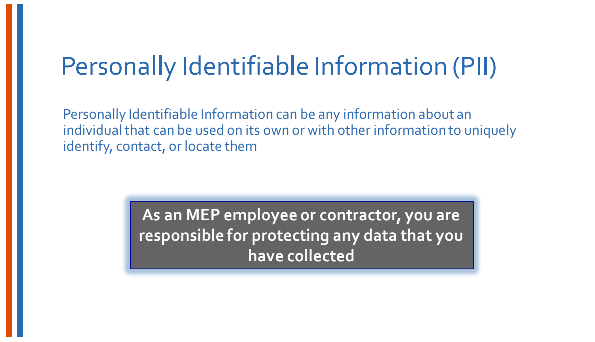
1

REVIEW

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

NEW YORK STATE MIGRANT EDUCATION PROGRAM

2



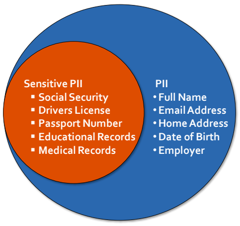
Personally Identifiable Information (PII)

Personally Identifiable Information can be any information about an individual that can be used on its own or with other information to uniquely identify, contact, or locate them

As an MEP employee or contractor, you are responsible for protecting any data that you have collected

3

Examples of PII



Sensitive PII
- Social Security
- Drivers License
- Passport Number
- Educational Records
- Medical Records

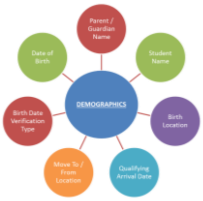
PII
- Full Name
- Email Address
- Home Address
- Date of Birth
- Employer

Combining pieces of PII data could result in a set of information that is uniquely identifiable

4

Migrant Student Data

- Migrant student information collected through the Certificate of Eligibility (COE) includes Sensitive PII
- Academic records associated with a migrant student are considered Sensitive PII



DEMOGRAPHICS

Parent / Guardian Name

Student Name

Birth Location

Qualifying Arrival Date

Move To / From Location

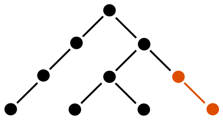
Birth Date Verification Type

Date of Birth

5

Principle of Least Privilege

This is the principle of granting the least amount of access necessary to perform one's job duties. Following the Principle of Least Privilege better safeguards the system data against possible compromise. In New York, student data is only granted to the employees who work with those students



6

Family Educational Rights and Privacy Act (FERPA)

- Passed in 1974
- Allows students to request their own records from schools
- **Protects the disclosure of student PII and educational records without consent**
- Exempts certain institutions from release consent requirements

7

FERPA Exceptions

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for, or on behalf of, the school

Source: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

8

FERPA Exceptions (continued)

- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies
- State and local authorities within a juvenile justice system pursuant to specific state law

Source: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

9

Parent's Bill of Rights

- NYSED has required a "parent's bill of rights" to explain what privileges parents have to access their children's data.
- This bill of rights is posted on nysmigrant.org/billofrights
- The rights can be summarized as:
  - Parent's have the right to review their child's education record
  - An educational agency must verify the identity of the requesting parent
  - These requests must go directly to the educational agency, and not to a third party
  - An educational agency must inform the parent of this right annually
  - The educational agency must fulfill this request within 45 days
  - The records may be sent electronically if the parent requests, as long as they follow proper security requirements

10

SECURITY TOOLKIT

USERS | DEVICES | INTERNET

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

11

The Three "C"s of Security

Secure conduct

Secure computers

Secure communications

12

Secure Conduct
Thinking secure when interacting with student data

Secure Computers
Ensuring all devices accessing student data are properly secured

Secure Communications
Utilizing secure methods to connect and send data over the internet

13

Conduct: Thinking Secure

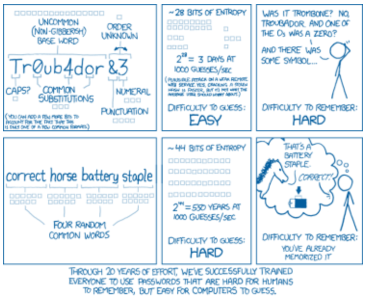
- Ensure only FERPA authorized parties have access to protected information
- Ensure NYS Migrant Education information is not released without consent

14

Conduct: Thinking Secure

- Request to use two-factor authentication whenever it is available
- **Never** share your account passwords or passphrases with anyone else. Users are responsible for all actions taken with their credentials
- Instead of a password, consider using a passphrase
  - Passphrases use combinations of words that are easy to remember, but difficult for a computer to guess

15


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Credit: xkcd

16

Please give me coffee?

17

Conduct: Thinking Secure

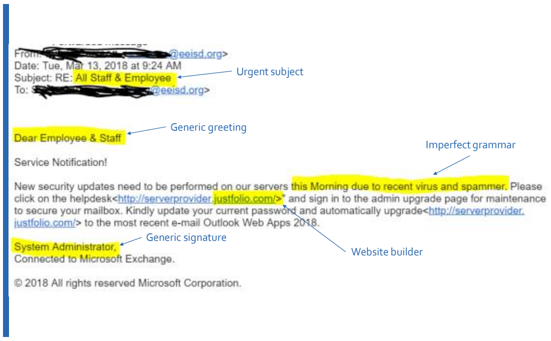
- Consider using a password manager
  - These will generate and remember unique passwords for all your accounts
  - Reduces the number of passphrases that you need to remember
  - Uses one master passphrase that **cannot** be reset if forgotten

18

Conduct: Thinking Secure

- Be aware of phishing scams
- Phishing scam emails attempt to trick you into giving up your password or other private information
- Phishing scam emails often try to create a sense of urgency, and inform you that you must act quickly otherwise something bad will happen to you

19



From: [redacted]@eeisd.org>
Date: Tue, Mar 13, 2018 at 9:24 AM
Subject: RE: All Staff & Employee
To: [redacted]@eeisd.org>

Dear Employee & Staff

Service Notification!

New security updates need to be performed on our servers this Morning due to recent virus and spammer. Please click on the helpdesk<http://serverprovider.justfolio.com/>" and sign in to the admin upgrade page for maintenance to secure your mailbox. Kindly update your current password and automatically upgrade<http://serverprovider.justfolio.com/> to the most recent e-mail Outlook Web Apps 2018.

System Administrator,
Connected to Microsoft Exchange.

© 2018 All rights reserved Microsoft Corporation.

20

Conduct: Thinking Secure

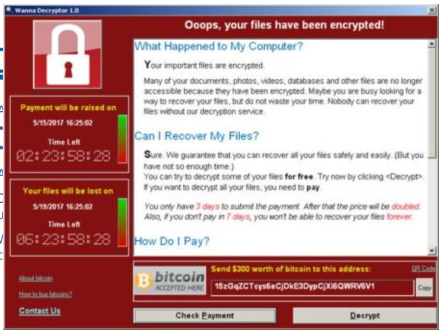
- Be aware of social engineering scams
  - Social engineering phone calls often come unprompted from an individual claiming to represent a large organization, such as Microsoft, who are calling with regards to an issue they have found on your computer
  - They will often attempt to direct you to websites that request your credit card number, account information, or access to your computer
  - Stop. Think. Ask the representative very simple questions that they would know if they worked for your organization. If they cannot answer, hang up

21

Computers: Device Security

- All devices containing PII should use full disk encryption
  - Bitlocker for Windows and for USB drives containing PII
  - FileVault for MacOS
- All devices used for work should have antivirus installed
- Do not leave devices out in a place where they may be stolen, such as an unattended car seat. Instead, store them somewhere out of sight.
- Work documents should be securely backed up on a network drive or a cloud platform so they can be restored if destroyed

22



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**.

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:

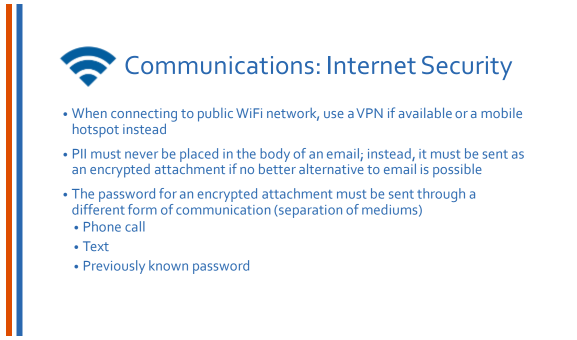
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

23

Computers: Device Security

Devices with Smart Assistants such as Siri, Alexa, or the Google Assistant, are configured to constantly listen for commands. It is best practice to use the "mute" feature on any of these devices while at work, particularly when any Personally Identifiable Information is being discussed.

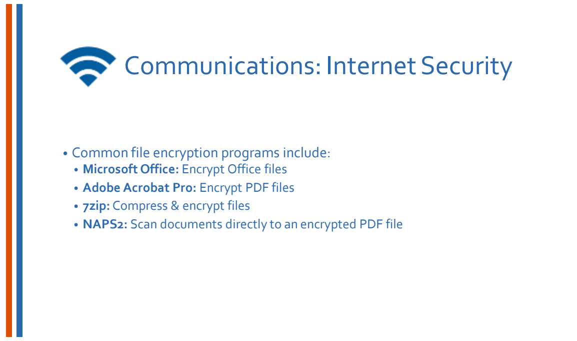
24



Communications: Internet Security

- When connecting to public WiFi network, use a VPN if available or a mobile hotspot instead
- PII must never be placed in the body of an email; instead, it must be sent as an encrypted attachment if no better alternative to email is possible
- The password for an encrypted attachment must be sent through a different form of communication (separation of mediums)
  - Phone call
  - Text
  - Previously known password

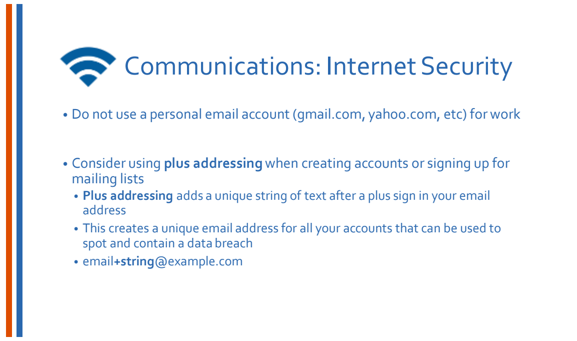
25



Communications: Internet Security

- Common file encryption programs include:
  - **Microsoft Office:** Encrypt Office files
  - **Adobe Acrobat Pro:** Encrypt PDF files
  - **7zip:** Compress & encrypt files
  - **NAPS2:** Scan documents directly to an encrypted PDF file

26



Communications: Internet Security

- Do not use a personal email account (gmail.com, yahoo.com, etc) for work
- Consider using **plus addressing** when creating accounts or signing up for mailing lists
  - **Plus addressing** adds a unique string of text after a plus sign in your email address
  - This creates a unique email address for all your accounts that can be used to spot and contain a data breach
  - email**+string**@example.com

27

QUESTION

"Can I just send the password in a second email?"

NO

28

Communications: Internet Security

- **Discuss:** what if I do not have another way to contact the individual?
- Include a confidentiality notice at the bottom of emails containing such attachments or information

29

Confidentiality Notice

"This electronic message is intended to be for the use only of the named recipient, and may contain information from the [organization] that is confidential or privileged, or protected FERPA. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately, either by contacting the sender at the electronic mail address noted above or calling the [organization] at [phone number], and delete and destroy all copies of this message. Thank you"

30

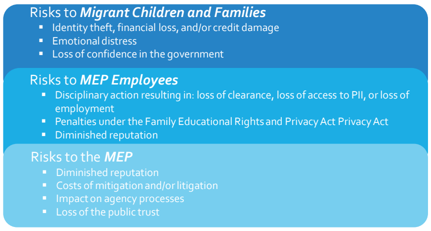
BREACH OF DATA

RISKS | CAUSES | REPORTING

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

31

Risks of improper handling



Risks to ***Migrant Children and Families***

- Identity theft, financial loss, and/or credit damage
- Emotional distress
- Loss of confidence in the government

Risks to ***MEP Employees***

- Disciplinary action resulting in: loss of clearance, loss of access to PII, or loss of employment
- Penalties under the Family Educational Rights and Privacy Act Privacy Act
- Diminished reputation

Risks to the ***MEP***

- Diminished reputation
- Costs of mitigation and/or litigation
- Impact on agency processes
- Loss of the public trust

32

Causes

- Can be a simple mistake, such as sending an email with PII to the wrong recipient
- Can be the result of a compromised account or device
- Theft of device
- Lack of encryption
- Many more

- Better safe than sorry- report any warning signs

33

Reporting

- Step 1: Contain the breach
- Step 2: Contact immediate supervisor
- Step 3: Contact the ID&R / MIS2000 Director
- Step 4: Document the breach

- On many occasions, the ID&R / MIS2000 Director might request that you participate in a detailed evaluation of the events leading to the breach for official records, prevention, and other uses

34

ENCRYPTION TOOLS

MICROSOFT OFFICE | 7-ZIP

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

35

Microsoft Office

Add a password to any Office file with this built-in encryption utility

W X P O N

36

7-zip

Encrypt any file, not just .PDFs!

37

Online Guide

All encryption steps can be found online for future reference at www.nysmigrant.org/encryption

38

What can you do right now?

- Turn on multifactor authentication for all your accounts
- Start using a passphrase for your next account
- Find a password manager that is right for you
- See if a VPN is available to you through your organization

39

QUESTIONS?

THANK YOU FOR ATTENDING!

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

40