Cybersecurity

What, Why and How

Whole Child ● Whole School ● Whole Community

What is Personally Identifiable Information (PII)?

The U.S. Government Accountability Office defines Personally Identifiable Information as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Examples of relevant Personally Identifiable Information include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, or driver's license number
- Address information, such as street address or email address
- Telephone numbers, including mobile, business, and personal phone numbers
- Information about an individual that can be linked to one of the above, including date of birth, place of birth, race, employment information, educational information, etc.

Password Construction

A good password adheres to as many of the following guidelines as your system will accommodate

1- Do not use familiar names - yourself, spouse, children, pets names…

2- Avoid using commonly known facts about yourself - Birthday, hobbies, favorite sports teams

3- Do not use words found in the dictionary - Programs found on the internet are designed to crack passwords by checking dictionaries

4- use at least eight (8) characters

5- utilize both letters and numbers

6- use special characters if possible (!@#$%&)

7- use upper and lower case letters if possible

8- combing misspelled words- by misspelling words you avoid the "dictionary" attack

Tips For Creating Effective Passwords

Compound words that we use everyday are easy to remember.
Mix them up with numbers and special characters.

bayz@ba11 (baseball)

gra$$#hoppr (Grasshopper)

Tips For Creating Effective Passwords

Using the first letter of each word in a phrase -
at least 8 words in the phrase

Lincoln's Four Score and 7 Years ago = L4s&7Yrsa

I love watching puppies all day long, too = iLwpupsAdL2

Gee, what I would give for a really good password=Gwlwg4argp

Back

Create a password with these ideas.....

Respond at **PollEv.com/lisaward933**

Answers to this poll are anonymous

Top

No responses received yet. They will appear here...

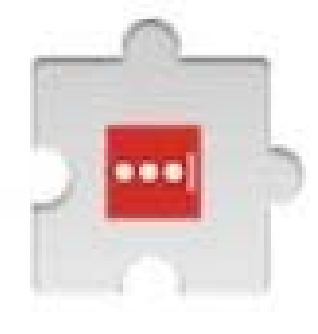
Poll Everywhere

Logout

Password management

- Do not share your password with anyone
- Never write down your password
- Do not store your password in a computer file
- When receiving technical assistance, enter your password instead of telling it to the technology staff
- If you ever receive a telephone call from someone claiming to need your password, report it

There’s an APP for that!



Last Pass - Only remember one password - your LastPass master password. Save all your usernames and passwords to LastPass, and it will autologin to your sites and sync your passwords everywhere you need them.

All Mobile devices available

https://chrome.google.com/webstore/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd?utm_source=chrome-ntp-icon

PC security

- Always use a security cable or locking device
- Lock your office door when leaving
- Lock away laptops, tablets overnight

On the road- 400,000 laptops are stolen every year

Decoys use tactics….help for a stranger
While using a phone in a public area, you may “look away”

Unauthorized access - configure a password protect screen saver

Set the screen saver password in Windows Vista, 7, 8, and 10

•Press the **Windows** key, type Change **screen saver**, then press Enter.
•In the **Screen Saver** Settings window, check the box On resume, display logon screen (A).

Logout of the system when you are finished working

- Press Ctrl+Alt+Del and choose the option to **Sign out**.
- Click Start and on the top of the Start Menu click your name and choose **Sign out**.
- Press Ctrl+Alt+Del and choose the option to **Sign out**.
- From the **Windows** 8.1 Start Screen click your profile icon and choose the **Sign out** option as shown in the picture.

Utilize a power-on password

This is an article walking thorough the steps….suggest there is a "techie" person available.

https://www.techwalla.com/articles/how-to-add-a-power-on-password-to-a-computer

How People Try To Get INFORMATION

Social Engineering

A social engineer is a person that will deceive or con others into divulging information that they wouldn't normally share.

It is one of the most commonly used methods of hacking.

One of the main things a social engineer counts on is our natural instinct as humans to be helpful to others.

Defending against a social engineering attempt is not easy.

Usually you won't know when it occurs until it is too late.

There are a few things you can do that might help.

If someone phones or appears and asks you for information that you know is confidential company, client or personal information, do not be afraid to ask them a few questions yourself.

By Phone:

•Ask for the correct spelling of the caller's name.
•Ask for a number where you can return the call.
•Ask why the information is needed.
•Ask who has authorized the request and let the caller know that you will verify the authorization.

In person:

•Ask for some identification.
•Ask who has authorized this request so you may verify the authorization.
•If you are not authorized to provide that information, offer to locate the correct person.
•Seek assistance if you are unsure.

Dumpster diving

Flash drive infiltration - never plug in an unknown flash drive

Phishing - email messages that are sent in an attempt to fool the recipient into providing personal or private information

Disguised - eBay, PayPal
Verify account- URL and "from" address

Reply Reply All Forward IM

Tue 6/12/2018 10:37 AM

Amazon Feedback <Tree-Basher@treebasher.com>

$100 Amazon Survey

Congratulations !

You're eligible to participate in a quick survey about Amazon! A few minutes of your time will earn you a *$100 Reward!*

Don't waste another *second!* This opportunity will be **GONE** before you know it!

All you need to do is tell us what you think about Amazon's Shopping Experience and this **$100 Reward** could be yours!

Claim Your Reward!

Social Networking is 10 times more effective than email to distribute malware

https://www.facebook.com/

Mobile Security

113 cell phones are lost or stolen every minute in the us alone

- Physical security
- Passwords
- Malware
- Wireless connections

Securing paper documents

How do identity thieves get access to our documents? They steal them…from our desks, our computer screens, our carts, our lading docks, our storage spaces and our trash.

Most sensitive data is taken from information being left in an unlocked cabinet, discarded inappropriately or left lying around.

Be aware of the confidential information contained in documents you work with.

If a document is electronic, consider whether it needs to be printed. If so, limit the number of copies of the document.

The fewer Paper documents the more secure we will be.

When document are not needed anymore, discarding them in regular trash or recycling boxes is inappropriate. Locate a “confidential shred container or shred the document yourself.

Only discuss personal information with individuals that need to know for business purposes. Be cautious about disclosing information over the phone….who are you really talking to???

60 % of unauthorized data access in from co-workers, lock your pc when you leave it. Do not give someone else the opportunity to use your pc without your knowledge.

Logout when you leave your computer…even for a moment

A simple rule to safeguard your laptop is treat it as money…keep it safe from loss. While on public transportation or Taxi/shuttles never place it on the floor. Keep it in your lap.

When sending emails regarding migrant families or individuals, only use a Unique ID number, such as those assigned by MSIX or MIS2000, to refer to them. Do not include any other forms of Personal Identifiable Information (PII), such as their first name, in the body of your email.

If Personally Identifiable Information (PII) needs to be sent over email, it should be sent as a password-protected attachment using the tools available in the Microsoft Office suite of applications, or by using a zipping tool such as 7-zip. This password should NEVER be included in the email, and should instead be sent to the recipient through alternative means, such as a phone call.

Password Protect MS Office Windows

Step by Step directions for 7-zip protection – Windows and MAC

Password Protect MS office MAC

What to do if you think anything has been compromised?

If it is suspected that a workstation computer has been compromised, or there is a threat that Personally Identifiable Information (PII) may have been stolen from the workstation computer, then the ***workstation computer should be immediately disconnected from the internet*** through appropriate means.

The supervisor should be immediately notified, and the workstation computer should remain ***powered on*** if possible while disconnected from the internet.


Q&A

Classrooms In Action

One Stop Resource Shop

www.ilclassroomsinaction.org

Tools and Resources for

ELA
MATH
Science
Social Science
Social Emotional Learning
Technology
Fine Arts

lkward2@ilstu.edu

Whole Child ● Whole School ● Whole Community