LESSON PLAN
FOR KIDS 7-13 yrs.
Cybersecurity and Digital Safety

CYBERAMA

OBJECTIVE

GOAL: Increase awareness cybersecurity and digital safety

OBJECTIVE: Complete interactive lesson plan for kids

EST. TIME TO COMPLETE: 50-60 minutes

INTENDED AUDIENCE: Kids ages 7 – 13, or grades 2-7

TOPICS COVERED

1. Password Strength
2. Personally Identifiable Information (PII)
3. Social Engineering
4. Malware
5. Cyberbullying

Printables:
Quiz, word search, crossword puzzle

CYBERAMA

LESSON 1 PASSWORD STRENGTH

How strong is your password? Time it takes a hacker to guess your password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2 k years	34 k years
13	4 minutes	1 year	16 k years	1000 k years	2 m years
14	41 minutes	51 years	800 k years	9 m years	200 m years
15	6 hours	1 k years	43 m years	600 m years	15 bn years
16	2 days	34 k years	2 bn years	37 bn years	11 n years
17	4 weeks	800 k years	100 bn years	2 tb years	93 tn years
18	9 months	23 m years	6 tn years	100 tn years	7 qd years

Source: HowSecureIsMyPassword.net

CYBERAMA

LESSON 1 PASSWORD STRENGTH

How to choose your password? Here's one way to set a strong password

Step 1: Select three things that are unique to you
Example: Football, Jelly, Blue

Step 2: Now combine the three things, and keep capital letters
FootballJellyBlue

Step 3: Replace a few letters with special characters
F00tb@llJellyBlue

Step 4: Add numbers in between or in the end
F00tb@ll5Jelly7Blue3

Viola, a strong password you can remember, and others can't easily guess!

Step 5: Use variations of this password for different applications
F00tb@ll5Jelly7Blue3Sc or F00tb@ll5Jelly7Blue3fb

CYBERAMA

LESSON 1 PASSWORD STRENGTH

Which of these passwords are strong, and which ones weak? Why?

a. Password123

b. QwertyComplex

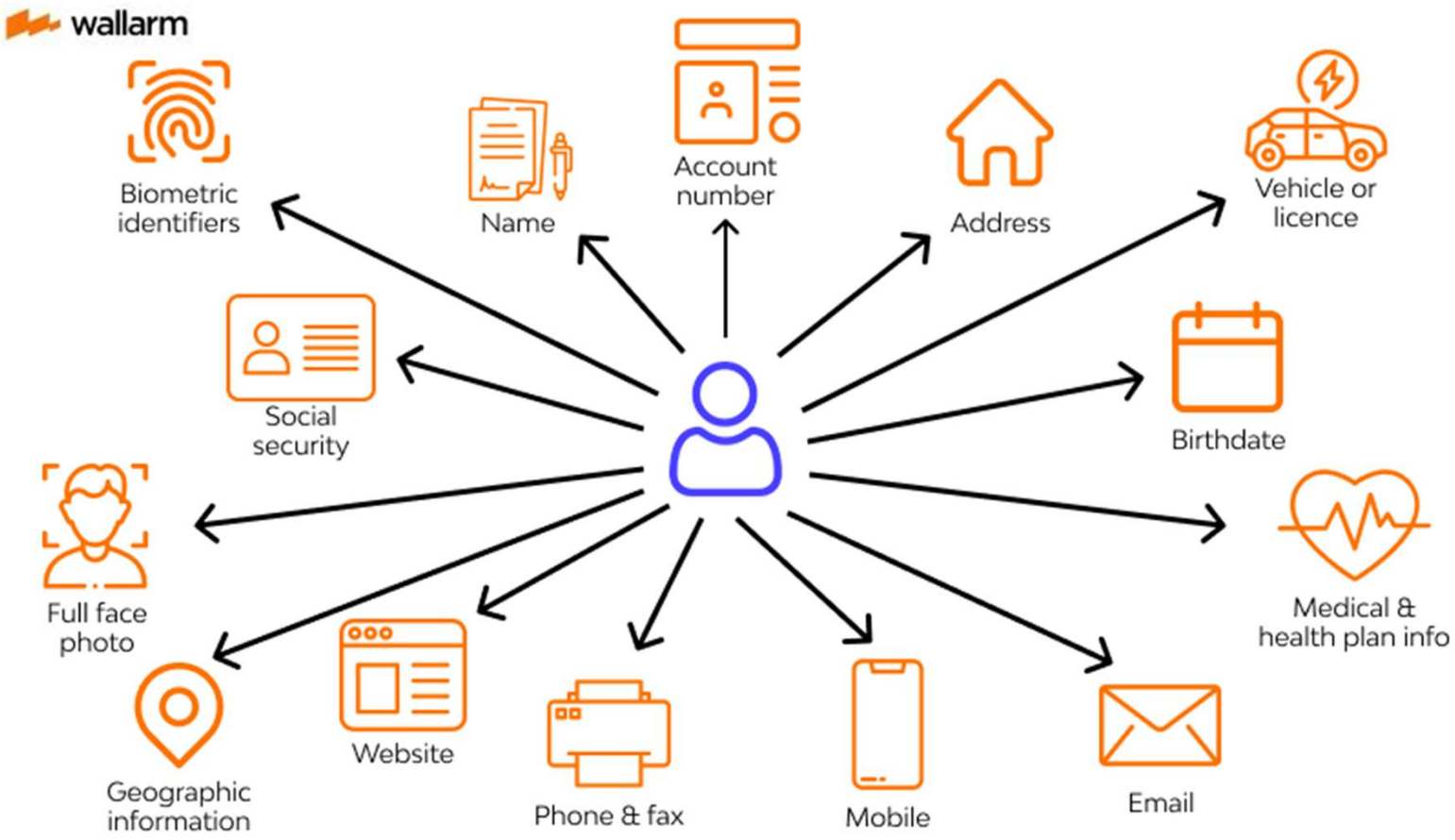
c. I3L0ve4C0rnD0g5!

d. Str0ngp@@ssw0rd*

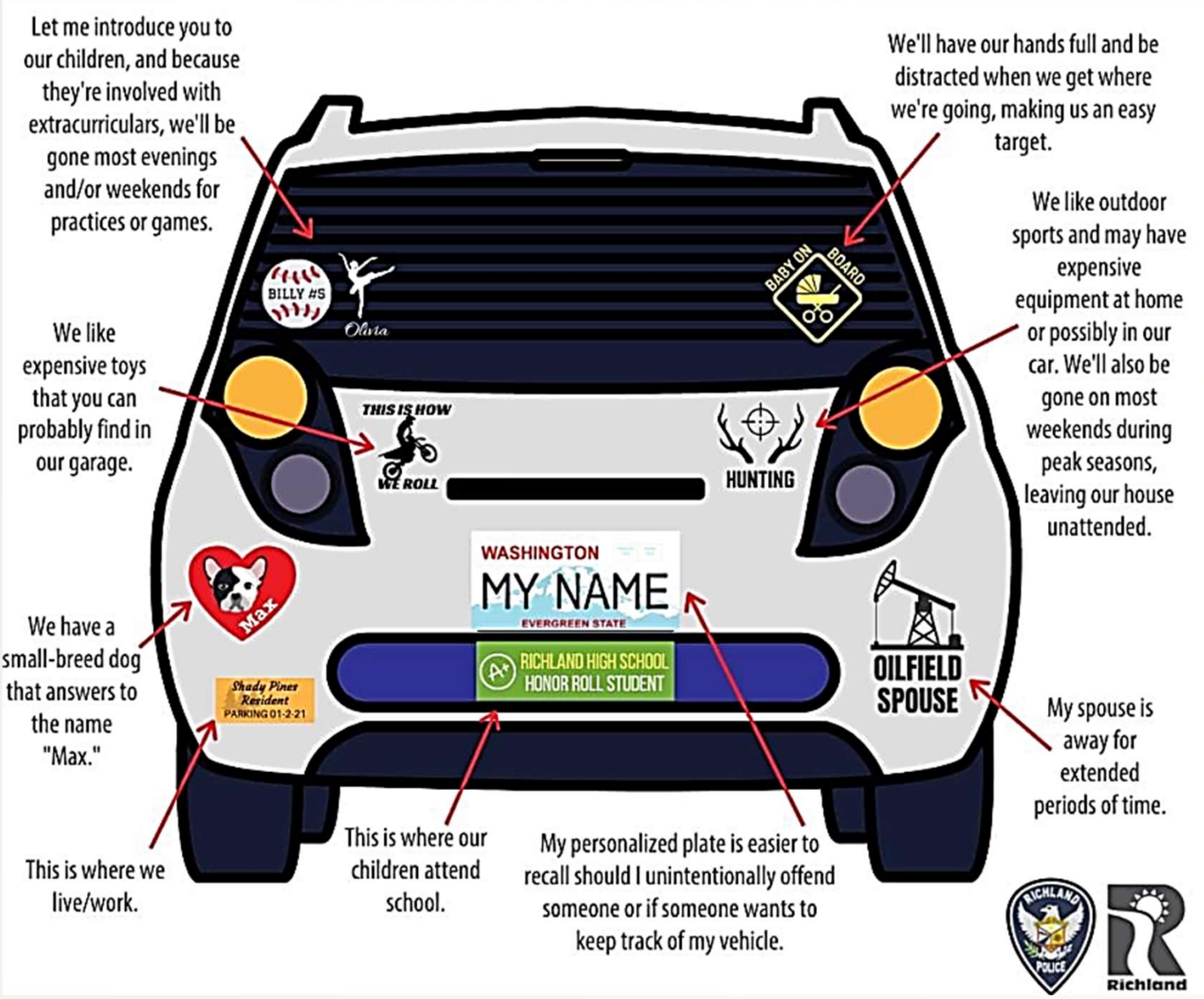
More password tips:

- Avoid real words or phrases
- Never use personal information such as name, pet name or phone numbers
- Never repeat passwords across accounts
- Protect passwords, never share them
- If writing or typing passwords, use hints instead of the entire password
- Password threats include: Dictionary attacks, password spraying and keylogging

LESSON 2 – PERSONALLY IDENTIFIIABLE INFORMATION (PII)



LESSON 2 – PERSONALLY IDENTIFIIABLE INFORMATION (PII)



Consequences of revealing PII: Identity theft, doxing (or doxxing0, loss of privacy, blackmail

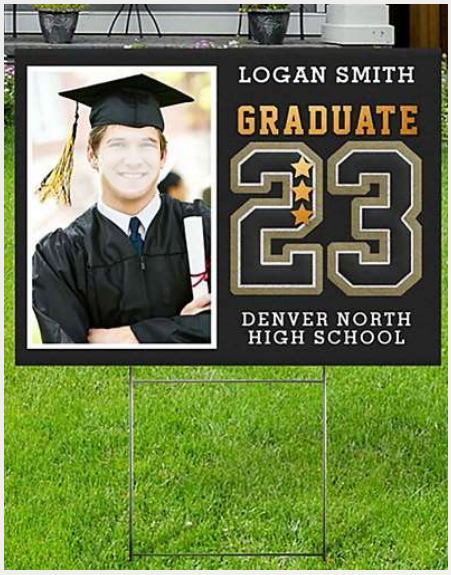
Source: Richland Police

LESSON 2 – PERSONALLY IDENTIFIIABLE INFORMATION (PII)

PII or not?	Yes	No
First name		
Full name		
Birthday		
Gender		
Place of birth		
Place of residence		
Pet name		
Password		
Home address		
School name		
School ID #		
School address		
Parent's names		
Sibling's names		
Parent's phone number		
Pictures in Social media		

LESSON 2 – PERSONALLY IDENTIFIIABLE INFORMATION (PII)

Note down what all PII each of these pictures is revealing.

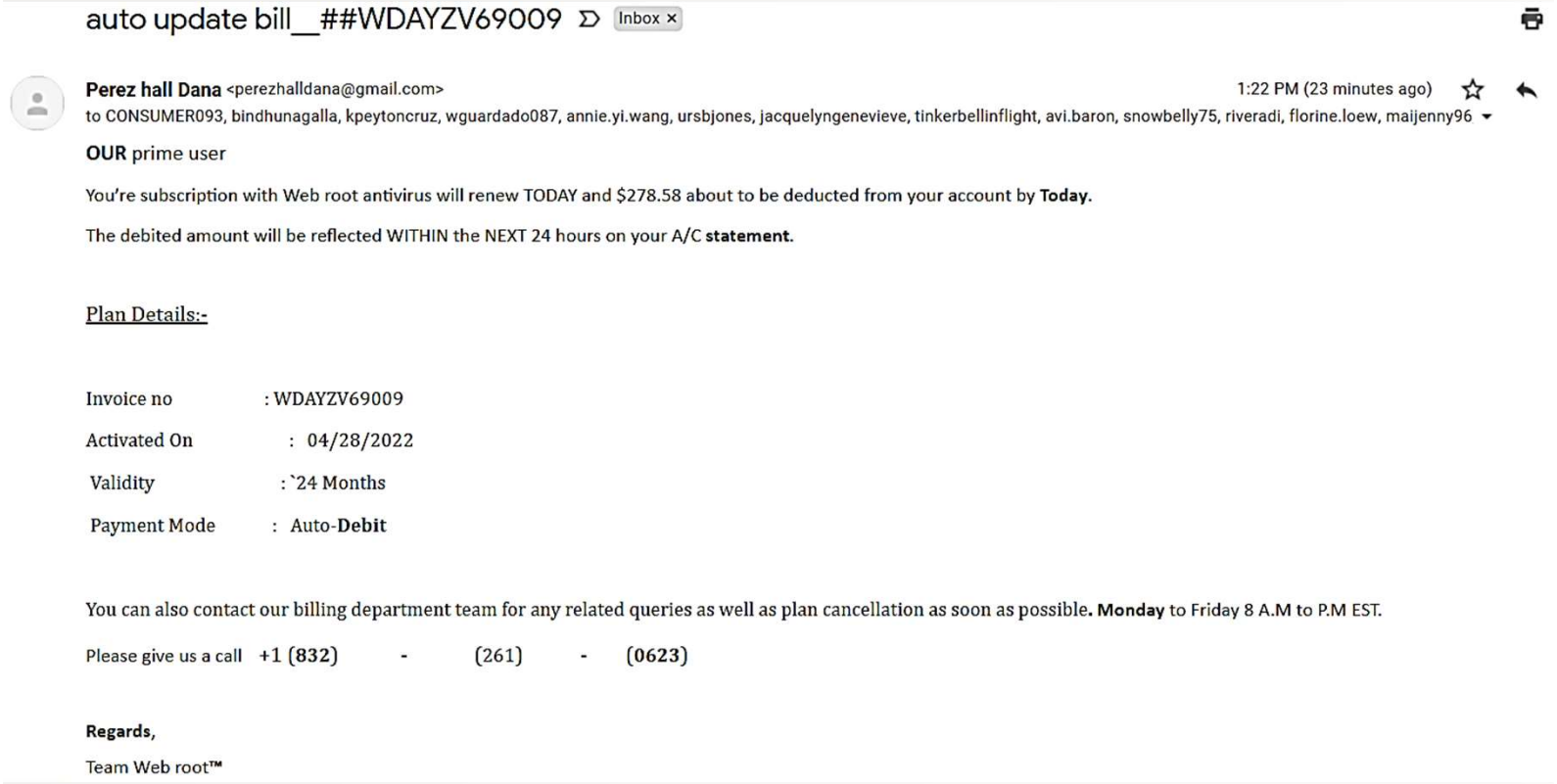


Source: Personal Creations, YouTube, Nintendo game, Pinterest

LESSON 3 – SOCIAL ENGINEERING

Social Engineering refers to techniques used to bad actors to manipulate you into revealing sensitive information such as your PII.

Below is an example of a phishing email. Identify five red flags which should serve as warnings to avoid clicking any links.



auto update bill__##WDAYZV69009 Inbox ×

Perez hall Dana <perezhalldana@gmail.com> 1:22 PM (23 minutes ago)

to CONSUMER093, bindhunagalla, kpeytoncruz, wguardado087, annie.yi.wang, ursbjones, jacquelyngenevieve, tinkerbellinflight, avi.baron, snowbelly75, riveradi, florine.loew, maijenny96

OUR prime user

You're subscription with Web root antivirus will renew TODAY and $278.58 about to be deducted from your account by **Today.**

The debited amount will be reflected WITHIN the NEXT 24 hours on your A/C **statement.**

Plan Details:-

Invoice no : WDAYZV69009

Activated On : 04/28/2022

Validity : `24 Months

Payment Mode : Auto-**Debit**

You can also contact our billing department team for any related queries as well as plan cancellation as soon as possible. **Monday** to Friday 8 A.M to P.M EST.

Please give us a call +1 **(832)** - (261) - **(0623)**

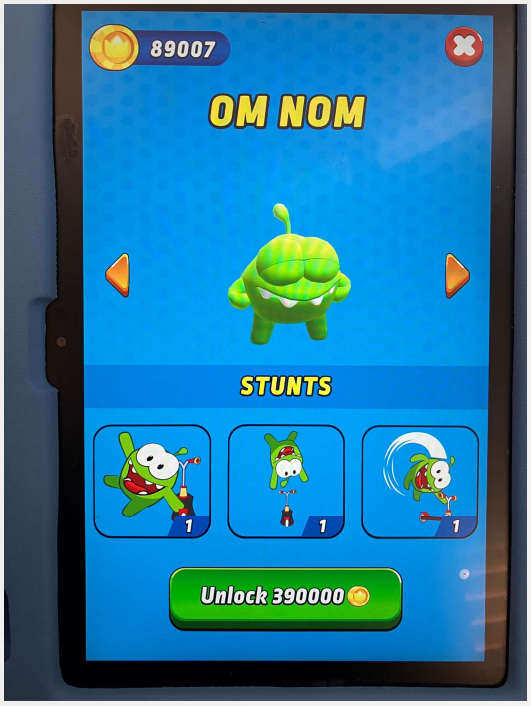
Regards,

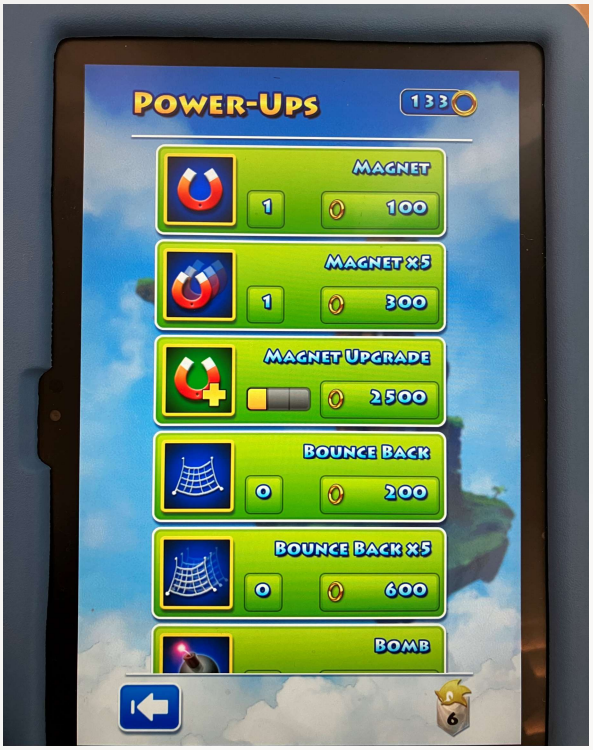
Team Web root™

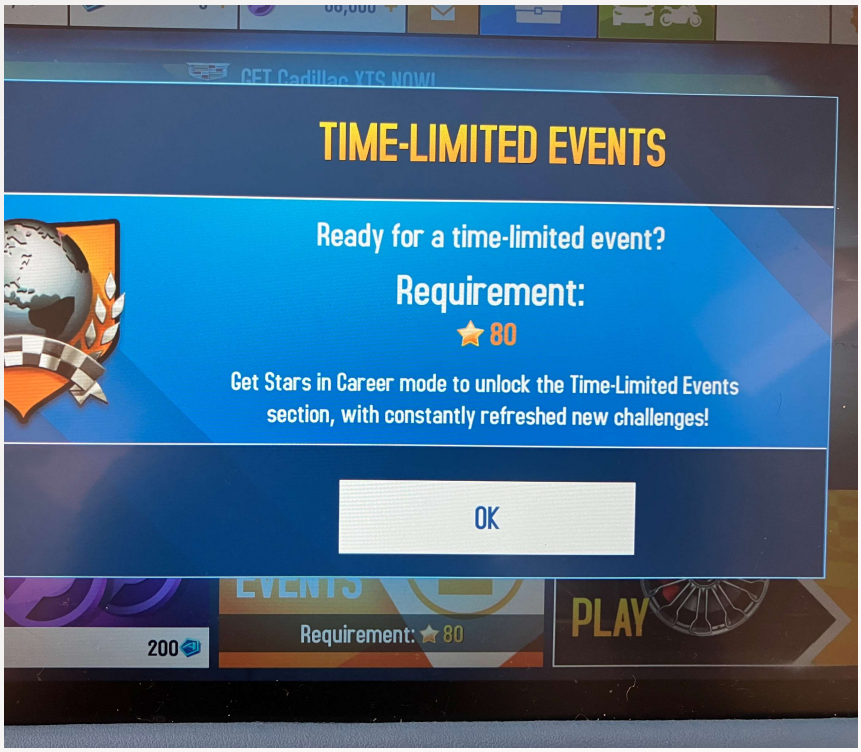
PRO TIP: Pay attention to logos in emails, sender's email ID, shortened hyperlinks, typos, request for PII and urgencies.

LESSON 3 – SOCIAL ENGINEERING

To click or not to click







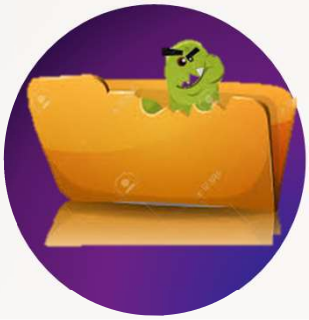
CYBERAMA

LESSON 4 – MALWARE

Virus – Most common type of malware, can erase data on device and spread by infecting files

Worm – Harmful computer program that multiplies itself and spreads to other computers

Spyware – Harmful computer programs that spy on our online activities without our knowledge



Adware – Harmful computer programs that are displayed as ads or free offers

Ransomware – Harmful computer programs that block our computers until we pay money (or emotional ransom)

LESSON 4 – MALWARE

1. You notice that your tablet is suddenly running slow. The next day, some of your files are missing. Two days later, your tablet completely stops working. A day later, your sibling's tablet which was connected to the same Internet network as yours, also stops working. What type of malware could have affected your tablet?

a. Virus b. Worm c. Adware d. Spyware e. Ransomware

2. You turn on your tablet, and are unable to logon. You get a message that your files are locked (or encrypted) and that you need to pay a large sum of money to unlock (or decrypt) your files. What type of malware is this?

a. Virus b. Worm c. Adware d. Spyware e. Ransomware

LESSON 4 – MALWARE

3. Your friend uses the Internet search engine to look for video games. A particular page asks him/ her to Accept Cookies to improve performance and show relevant searches. An hour later, your friend starts seeing numerous ads of videogames. What type of malware is this?

a. Virus b. Worm c. Adware d. Spyware e. Ransomware

4. A pop-up appears on your tablet asking you to download an Antivirus Software, since a virus has been detected and the software will help contain the virus from spreading. You click the Anti-virus software, after which your tablet stops working. What type of malware could this be?

a. Virus b. Worm c. Adware d. Spyware e. Ransomware

LESSON 6 – CYBERBULLYING

Tell a trusted adult if someone on the Internet makes you uncomfortable or says something that worries you. A trusted adult is ideally a family member or teacher, 18 years or older, whom you can share stuff to without fear of being judged.

Activity:

Step 1: Write down the names of 4 trusted adults in your life.

Step 2: Draw pictures of them below their names.

TEST YOUR KNOWLEDGE

1. You're playing a game in your personal computer (not school's, with parents' approval in designated screen time). You're being asked to create a name. Which of the following would you choose?

a. Your real name **b. A fake name**
c. Ask your parents **d. Stop playing the game**

2. Once you enter the name, you're being asked to create a secure password. Which of the following should you choose as an example?

a. Password123 **b. I3L0ve4C0rnD0g5!**
c. qwertycomplex **d. Str0ngp@@ssw0rd***

3. You're playing a learning game recommended by school. Once you create an account, you pass 3 levels. The game gives you the option to create a custom avatar that looks just like you. You need money to buy custom avatar. What should you do?

a. Ask your parents to buy the avatar b. Press close button to not buy avatar c. Ask your parents what you should do

TEST YOUR KNOWLEDGE

4. You have a sleepover at a friend's place. You friend says he/ she will think you're cool only if you play the 'online' version of the game instead of the offline version that's not connected to the internet. You really want your friend to like you. What should you do?

a. Play the internet version of the game
b. Ask your parent what you should do
c. Explain to friend that the online version is not the safest for kids

5. The game prompts a message to click "Claim Offer" to buy stickers with your name that is available for purchase in Amazon.com. What should you do?

a. Click the "Claim Offer" button b. Ask parents what to do c. Close the pop-up message

6. While playing in game, you suddenly get a pop-up with a chat message from someone asking you to friends with them. What should you do?

a. Never chat with strangers and close the pop-up b. Click 'Yes' to chat and make a new friend c. Ask parent what you should do

THE FUN DOESN'T STOP HERE!

Visit Cyberama.org for more resources include a FREE web based game to test your cybersecurity knowledge

CYBERAMA

INSTRUCTIONS FOR TEACHERS/ EDUCATORS

1. Password Strength

- Page 3 (Password complexity table): Explain that having a long and complex password or a passphrase with a mix of upper- and lower-case letters, numbers and symbols will make it difficult for a bad actor to break a password and hack into one's account. Ask students/ kids if they can name a few symbols/ special characters such as !@#$* that look similar to letters (Example, $ in place of letter "S", @ in place of letter "a", 3 in place of letter "e", zero in place of letter "O". Suggest that students can use the number 1 to replace the letters "L" or "I" as long as they can remember.
- Page 4 (Example for setting a password): Ask a student/ kid for their favorite color, then ask another student for their favorite food and one more student for their favorite sport. Then have them write the three words together. You could make this interactive by asking students to call out which letters can be replaced with which numbers. Suggest the students to use different combinations for various accounts or use passphrases. They could also use the same word combination with different numbers in between the words.
- Page 5 (Activity): Have the students complete the activity in 2 minutes.

INSTRUCTIONS FOR TEACHERS/ EDUCATORS

2. Personally Identifiable Information (PII)

- Page 6 (PII intro): Explain to students that PII is any information bad actors can use to identify and manipulate a person.
- Page 7 (Car): Ask students if it's safe to have stickers about the gymnastic class they go to or the school's name in the honor roll sticker at the back of their parents' car. Explain that such sensitive information can be used to trace kids' location as well as their families and that leaving a trail in the real world about PII is as dangerous as leaving a digital trail.
- Page 8: Have the students identify PII in 5 minutes. While various students would have different responses, call out one student each for 3 or 4 questions and ask them why they answered "Yes" or "No" for that PII. Explain that while exposing one PII may not be as harmful, bad actors can hack into someone's account having one or more PII of the same person.
- Page 9: Have the students/ your child write down PII revealed in each picture. Ask 3-4 students to share answers.

CYBERAMA

INSTRUCTIONS FOR TEACHERS/ EDUCATORS

3. Social Engineering

- Page 10: Talk about the importance and risk of leaving a digital trail in social media. Have the kids identify five red flags in the email. Ask 1 or 2 students to come up to the front of the class and share their responses.
- Answers: (1) Sender's email address (unknown sender), (2) Email addressed generically to "OUR prime user" (3) Urgencies ("TODAY", "NEXT 24 hours"), (4) Typos and additional/ inconsistent spacing, (5) Request to contact a phone number, which is most likely a spam to get more PII from you such as financial information.
- Page 11: Talk to kids about examples of online games that ask them to power up or unlock points/ levels if they provide PII or their parents' credit card information to buy

INSTRUCTIONS FOR TEACHERS/ EDUCATORS

4. Malware

- Page 12: Read out and explain the different types of malware. Explain that the main difference between a virus and a worm is that while both slow down a computer, tablet, or phone, a worm spreads across all devices connected to the network. For example, if a kid clicks a link while at home, which ends up downloading a piece of malware on their device, other devices, such as parents' computers and tablets, could also get infected with the malware since they're connected to the home Internet network.
- Pages 13 and 14: Answers to the Q&As: 1. b. Worm, 2. e. Ransomware, 3. c. Adware, 4. a. Virus

INSTRUCTIONS FOR TEACHERS/ EDUCATORS

5. Cyberbullying

- Page 15: Explain to kids that cyberbullying may take different forms, including offensive name-calling, spreading false rumors, intrusive questioning, physical threats, receiving explicit images, and having explicit images shared without permission. Encourage kids to reach a trusted adult if in fear of being bullied on the internet. A trusted adult is, ideally, a family member or teacher whom they can share stuff with without fear of being judged. They are typically 18 years of age or over.
- Pages 16 and 17: Answers to the Q&As: 1. b. Fake name, 2. b. or d. b. I3L0ve4C0rnD0g5! is more secure, as d. has is derived from the word “password” , 3. b. Press close button to not buy avatar or c. Ask your parents what you should do. This is a form of social engineering, asking kids to make their parents spend money. Also, it is not safe to reveal your image to create a custom avatar. 4. c. Explain to friend that the online version is not the safest for kids, 5. c. Close the pop-up message. Again, this is a form of social engineering, alluring you to spend on things you may not need, 6. a. Never chat with strangers and close the pop-up.