Digital Security

Introduction:

When we use any digital system - this can be our phones, tablets, computers we enter information about ourselves. This can be sensitive information about our families or very important information from our places of work. This also includes creative material like pictures and videos.

It is very important to protect our own data and the devices (phones, laptops etc, we use to access the digital world) and respect the security of other people’s data and devices. As the internet is a place where we are all connected, everyone needs to make sure they are being safe because one person’s weak security can affect everyone.

Digital security and cybersecurity do not mean complicated or difficult security systems. Sometimes the best solution can be very simple and not at all technical. It is also important to keep checking if our security systems are strong, as there may be new threats, especially on the internet.
Honey... It's mom, open the door.

Just a second.
It’s my house now.
NEXT DAY...

Honey. It's mom, open the door.

I should go look. Mom?... She didn't tell me she was coming by.

KNOCK KNOCK

OMG!
The little pig had an extra layer of security.

Two step authentication is using an extra layer of security for your account other than the password.

Usually it’s a code sent to your phone to confirm your login again. Two step authentication is better for safety.
Also, remember to add strong passwords.

What else can I do?

- Making sure to update security settings on social media profiles.
- Exercising caution when sharing personal information online.
- Staying away from unsafe websites, which could infect your devices.
- Having antivirus software; update it regularly.
- Avoiding unsafe downloads.
Lessons Learned

• Strong passwords are important to keep our accounts safe.

• Use two-factor authentication - this means instead of just one password you will be asked for another secret number which only you will know. This is a code sent to your phone or email account to confirm your login.

• Updating security settings on social media profiles (such as Facebook, Instagram etc) is crucial to keep your accounts safe.

• It is important to be careful when sharing personal information online.

• Stay away from unsafe websites that can infect or damage your devices.

• Avoid downloading software from unknown websites.

• Always use a virus guard and update it regularly.
FAKE NEWS

Story & Design: Poornima Meegammana  Artist: Trishan Fernandopulle
Fake News

Introduction:

One of the most important parts of digital literacy (this is the knowledge you have of digital systems) is not only finding information but also checking if that information is good and accurate. You must check if the place from where you received the information can be trusted.

Fake news is a popular phrase, but not a very helpful one to understand what is unreliable or incorrect information, because it can take different shapes and forms:

- Disinformation (deliberately spreading falsehoods)
- Misinformation (unknowingly spreading falsehoods)
- Malinformation (falsehoods spread with the intent of causing harm in society)

False information and images have been around for many many years. In the 21st century, however, the internet and the use of social media has made it much easier to create and/or share falsehoods. Some of these can cause real harm: they can affect society, bring about misunderstanding and quarrels among religious or racial groups, confuse voters at elections, and even threaten a peaceful society by encouraging violence.
Mmm... This smells really good.

Must be delicious.

I don’t want to share this.
Labu Kiribaath taste better on stemless Kanda leaves.

Can you go find some?

Where are these stemless kanda leaves?

No... It has a stem.

Kanda

Mmmm

No leaves here... I’m Hungry!
BURP

WHAT!

!*#@%!*#$$!!

!*#@%!*#$$!!

Help me up.

Rabbit attacks fox!
Fox is in Critical Condition.
The post went viral.

Can't let the Rabbit get away with this.

This is Wrong.

Hey Come see this.

I heard the fox is in the ICU.

Really?

Rabbit attacks fox?

PRESS CONFERENCE
They are on my side for the first time.
Innocent rabbit got arrested because of the false information shared. If the information you share is false, it can hurt someone.
Lessons Learned

Tips on how to spot fake news:

• Beware of stories that don’t make sense.
• Check the name of the news site that published it.
• Beware of fake website addresses.
• Look out for headlines which don’t match the story.
• Look for unusual spellings and mistakes.
• Be wary of headlines which are trying to make people angry.
• Look out for falsehoods spread by fake celebrity accounts.
• Google search the images.
• If you are unsure, double-check with a source you trust.
FOOTPRINT

Story & Design: Poornima Meegammana  Artist: Prabhashana Hasthidhara
Digital Footprint

Introduction:

Every day, whether we want to or not, most of us contribute to a growing picture of who we are online; a picture that is probably more public than we think.

Your digital footprint is all the stuff you leave behind as you use the internet. Comments on social media, Skype calls, app usage and email records. It's part of your online history and can be seen by other people.

This helps companies to find out about what you like and send you advertisements according to your likes, and helps employers to look into your background. Whatever you do online you might be leaving digital footprints behind.

You can learn more about digital footprints by visiting this link
https://www.internetsociety.org/tutorials/your-digital-footprint-matters/
A letter?

You passed the exam.

Wow, A Laptop?

Thank You! I love it.
He continued to create a bad digital footprint.
Did you apply for the prefectship?

Yes. My interview is tomorrow.
This is my dream.

We will let you know.

Impressive Resume.

Thank you.

Best candidate.

I like him.

But...

I checked on him. He has a very bad digital footprint.

Oh then we can’t make him a prefect!

Yes, it’s not good for the school.

Menura lost his prefectship because of the bad things he shared online.

What you put online is there forever.
Lessons Learned

Managing Footprint:

• Be yourself, but speak carefully and respectfully.

• Make sure to check your privacy settings.

• Keep a list of accounts and delete the ones you no longer use.

• Be careful about who has access to your information.

• Google yourself - you may be surprised at what you find.

• Remember that every time you send a message or put up a post, or picture, it is there forever.

• Use digital tools to manage your digital footprint.
DIGITAL WELL BEING
Digital Well Being

Introduction:

While we need digital tools and services for our day to day lives, we need to manage the ways in which we use them, to make sure they don’t affect our health - this includes both physical and mental health. Spending several hours each day looking at a digital screen, especially if you are seated, can lead to health problems.

Using digital tools and services over a long period of time can affect our minds and moods too and can even harm our relationships with other people.
Did you see? Spending too much time on your digital devices can cause serious physical problems. Your eyes, ears, neck and back can all be affected.

The girl in this story didn’t even realise how much her body was changing, until it was too late.
Lessons Learned

Actions to minimize health impacts of digital tools:

• Place your computer where there is enough lighting and minimal glare, about 20 to 30 inches (50cm to 76cm) away from your eyes.

• Take care of your eyes. Don’t forget to blink! We tend to blink less frequently than normal when using a computer.

• Take a 20-20-20 break for the eyes, i.e. staring at something at least 20 feet away for 20 seconds every 20 minutes.

• Don’t go to bed with your smartphone or any other gadget, on your bed or close to you. To make sure your sleeping patterns are not disturbed, turn off all your screens an hour or two before you go to bed and let your eyes rest.

• To avoid constantly looking down, raise your laptop to eye level by placing something under it.

• Do some exercises. While you’re studying or working, take short breaks to do some simple exercises.
HATE SPEECH

Story & Design: Poornima Meegammanasa  Artist: Akalanka Gamage
Hate Speech

Introduction:

Everyone has the right to share their thoughts and opinions. What is not allowed is using your right to speak out, to encourage violence against others. This is generally called hate speech.

Hate speech is found both offline and online, and while good and useful criticism is allowed, statements that can lead to real harm should be avoided altogether.
Yay! I won.

Maybe next time Fathima.
Guys is everyone safe?

Yah.. I called Abhi and Logan

This is so sad be careful guys

I heard a Muslim extremist group is responsible

Fathima do you know them?

What? No!! I don't know anything

So the movie is off right?

Yeah...Stay home these...
Logan posted that?

I can't believe they think like that.

I thought they are my friends.

Fathima
Are you sure you want to deactivate your account?

Eat something.
You can't stay in there all day.

I can't eat mom.
but why?

Where is Fathima?

I'm calling her now.

I texted her last week she didn't reply.

Yeah she has left the group too.

What Fathima’s friends shared hurt her.

Things you share may hurt someone you might not even think.
Lessons Learned

Responding to Hate speech online:

• **Don’t share it**
  It is wrong because someone can really get hurt because of the words you use. It can also affect you as it can potentially be traced back to you and get you in trouble. For example Menura and his digital footprint which cost him a prefectship.

• **Report it**
  Hate speech violates most sites community guidelines. That means it goes against how they function. This allows people to report others who are using hate speech, without the others knowing that you were the one who complained.

  Talk to an adult and ask if the page should be reported to the authorities.

• **Block it**
  You can block people who use hate speech from your social media accounts.

• **Call it out**
  You can make it clear that you do not agree with the post or status update. Speak against the content of the post and not the author. Call out false claims where possible with facts. Refer to reliable sources. Express your disbelief in a professional manner and avoid getting into a shouting match with insults.
DIGITAL ACTIVISM

Story & Design: Poornima Meegammana
Artist: Sugapratha Somaskantha Iyer
Digital Activism

Introduction:

Activism means taking up an issue in a peaceful manner, publicly with the aim of bringing about social or political change. The change that is expected can be at a community, national or even sometimes at the international level.

Digital activism (also known as cyberactivism) is a form of activism that uses the internet and other digital technologies as tools for awareness-raising and more importantly, action.
Government doesn't care
No response to our petition.
It's been a year.
They Still haven't built it.
Not getting my vote at the next election.

Wish we could do something.

Let's make a video about this
Yes.
We can post it online.
A year has lapsed since the bridge broke due to floods. Government doesn't seem to care. #fixthebridge

The post went viral.
24k Shares!

I'm losing support. I need these people for reelection.

Fix the Bridge
You can use your mobile phone and internet to draw attention to issues/problems in society and to campaign for solutions to your community’s problems.
Lessons Learned

Many successful online campaigners have found various creative strategies. Below are some examples:

**Online petitions:**
This is a great tool if the right response is received. Some online petitions have hundreds of thousands of people signing. When this is done governments and corporate entities can’t just ignore it and pretend otherwise.

**Hashtags:**
A good hashtag helps sort out the information you are sharing, and people can find messages with a specific theme on social media platforms such as Twitter, Instagram, Facebook, Reddit, and YouTube.
CYBER EXPLOITATION AND VIOLENCE

Story & Design: Poornima Meegammana
Artist: Trishan Fernandopulle
Cyber exploitation and Violence (CEV)

Cyberbullying is when someone bullies or harasses others on the internet using digital tools. Harmful bullying behaviors can include posting rumors, threats, or putting somebody’s personal information online without their consent. This includes being bullied because of your religion, language or your gender, etc.

If you are a victim of Cyberbullying, these are some of the things you can do:

• Inform an adult (your parents or your teacher).

• Report to the National Child Protection Authority (NCPA) if you are under 18.

• Report to the Cyber Crimes division of the Police Criminal Investigation Department (CID) if you are over 18.

• Report to the Sri Lanka Computer Emergency and Readiness Team (SL-CERT).

• Report to the relevant social media platform’s administrators.
This is Charuka. She is joining us from today.

Hello.

Hi Charuka.
Next Day

Who knows the answer?

$A^2 + B^2 = C^2$

It's Five

Good job Charuka

We have enough people

Hey can i join?
Good morning

This seat is taken
You are a loser.
No one wants to play with you.
Everyone hates you.
Go back to where you came from.
You suck.

You have no friends.
You are a loser.
Soo Ugly.

I found an old photo of you @Charuka.
I thought they are my friends.

I found a post of you.

Save post
View edit history
Embed
Turn on post notifications
Report

Mom Some kids are bullying me online.

What? do you know who it is?

I'm calling the principal.

Yes, I saved everything.
You could go to jail for this. You are lucky they don't want to go to the police.

I'm suspending the three of you.

Sorry Charuka.

Like Charuka, if you are being Cyberbullied keep evidence and inform a Parent or a Teacher you trust.

Cyber bullying and spreading hate online can have serious consequences.
Lessons Learned

• If you are being bullied, harassed online or blackmailed, take screenshots of what was said. This is important evidence.

• Keep a record of what has happened. Write down what was said, take screenshots, along with the date and time when the cyberbullying took place.
Digital Identity Theft

Introduction:

Identity theft can happen both online and offline. It is collecting personal information about someone without his or her consent and using that information for criminal activity. For example using the credit or debit card details of another person and spending money which doesn’t belong to them.

There are several ways in which somebody’s identity can be stolen, one of the ways is phishing. This method is used by criminals to pretend to be other organisations (like a bank or company) which makes you think you are being contacted by the actual bank/company. Usually this is done using email or SMS and will include asking people to enter personal financial details.
City Bank Alert

A transaction for LKR 100,000.00 has been credited to your account. Current account balance LKR 446,000.00

It's my lucky day...
Dear Mr. Thambil,

Congratulations!!!
As a loyal google chrome user you Have been randomly selected to receive a free Smartphone.

To receive your gift please pay the shipping fee of 12.95$.

Pay now at: http://chromeloyalty.com

Thank you,
Google chrome loyalty team

Wow! I won a phone

Yes!!!
All your money is mine

CLICK

http://chromeloyalty.com/Pay

CARD INFORMATION

Name on Card  K.M. Thambil
Card Number  4213 4785 6316 7531
CVV  231
Expiration Date  05/06/2020

Thank You
Your payment was successful
We will send you the Smartphone.
How could this happen?

City Bank Alert
A transaction for LKR 446,000.00 has been debited from your account. Current account balance LKR 0.00

Mr. Thambili lost all his savings because he trusted a phishing email and shared his personal information online.

Be careful when you provide personal information online.

All my money is gone.
Lessons Learned

Tips on safeguarding against phishing:

• Beware of accessing suspicious URLs that require you to enter your bank details.

• Keep track of your credit card and banking statements to check for any suspicious transactions.

• Use only secure websites for financial transactions. If you enter credit card information online to make a purchase, you should see a lock in your browser’s status bar, usually in the left corner. If you don’t see the lock, don’t enter your information.

• Don’t reply to emails or follow the links in emails claiming to be from reputable institutions like your bank or university that ask for personal information. Contact the institution in question via phone or their website about these emails.

• Use common sense. If an offer sounds too good to be true (“Just enter your credit card number for a free trip to Paris!”), it is likely to be a scam!

• Don’t send any personal information when using public WiFi. Public WiFi have low security and can be easily hacked.

• Look out for emails claiming to be from companies such as Norton Anti-Virus that prompt you to download something. Get in touch with the company on your own (do not reply to the email itself) to check if the information is true or not.