Erasmus+

Project funded by
Erasmus+ Programme

Polish - Lithuanian Cooperation

Be Careful on the Web

I Youth Exchange
25.06-04.07.2019
Murzasichle, Poland

II Youth Exchange
18.07-27.07.2019
Poronin, Poland

About the project

Today, more than half of the world's population uses the Internet. The idea for this project was born by hearing stories of people being cheated on the net. Youth in particular is vulnerable because young people are "on the web" all the time. To prevent this, we decided to prepare a special project aimed at instilling certain rules that will allow young people to use the Internet in a safe way. We want participants to be aware that every movement in the network leaves a trace and that we are not anonymous.
In an easy way, we may not notice when our data, passwords will be stolen and quickly used. The most important thing is to be able to distinguish between safe pages from those that are hacked. The youth participating in this project after the exchange are aware of the decisions they make on the network, pay attention to the websites, and above all, understand that the Internet is not only for entertainment, but also teaches many wise things. When discussing issues related to safety and caution in the network, young people had the opportunity to cooperate in groups, establish new contacts and acquire interpersonal skills that translate into the objectives of the Erasmus + programme.

The main goals of our project are:

- giving young people attitudes and values such as: tolerance, openness to other cultures, respect, a sense of European community;

- raising the language skills of the participants;

- promotion of the Erasmus + program and development opportunities that it offers to young people;

-

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

- integration of young people from partner countries and creation of strong partnerships between participating countries through the involvement of young people in all stages;

creating a guide on how to safely navigate the network;

- creating a spot depicting an example of online fraud;

- raising competences related to computer use.

A total of 64 people from Poland and Lithuania participated in the prepared project. In the course of the project, two youth exchanges was organized - Murzasichle - 25.06-04.07.2019 and Poronin 18-27.07.2019. Each exchange was attended by 32 project participants (15 people +1 leader from each country).

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Rules of safe Internet

Nowadays the Internet is a huge part of many people's everyday lives. Not only is it a source of entertainment and information but it can also be dangerous. However, not all information or users online are trustworthy. By getting into the habit of using good Internet safety practices, you can protect your information and identify for years to come.

Remember:

*** take control of your email - don't open or click on links in emails that tell sad stories, make unsolicited job offers, or promise lotto winnings**
*** use strong passwords - use a variety of letters, numbers and special characters - the longer and more complicated the better**
*** use antivirus software and keep it up to date - install antivirus software and spyware scanners that look for viruses, malware, and other malicious content.**

In the 21st century, the advent of social media platforms and online dating websites allow people to make connections with others over great distances. These days catfishing (the process of befriending or chatting with someone online, while using a fake identity) occurres more frequently than ever.

To protect yourself:

*** never give out your sensitive information to other users.**
*** don't leave yourself exposed.**
*** ask for proof of who they are - if they are reluctant to send a photo, you can promptly cut it off.**

To summarize, although the Internet is very beneficial nowadays, some rules are ought to be followed if you want to protect yourself from dangers.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Second Life

What is Second Life?

Second Life is an online virtual world, developed and owned by the San Francisco-based firm Linden Lab and launched on June 23, 2003. By 2013, Second Life had approximately one millio regular users; at the end of 2017 active user count totals "between 800,000 and 900,000". Second Life is similar to massively multiplayer online roleplaying games. Users, also called residents, create virtual representations of themselves, called avatars, and are able to interact with places, objects and other avatars. They can explore the world, meet other residents, socialize, participate in both individual and group activities, build, create, shop, and trade virtual property and services with one another. This game also has its own virtual currency, the Linden Dollar, which is exchangeable with real world currency.

What kind of problems Second Life causes?

- **People lose track of time.**
- **If you decided to invest a lot of money into this game, you basically lose them.**
- **This game consumes a lot of time, as a consequence, you are forgetting about your family, friends and other precious people.**
- **People get lost in virtual life and then can’t separate it from real life.**
- **Second Life is an addictive game, later on you can’t live without it.**
- **You can experience sexual harassment.**
- **There are a lot of other dangers: catfishing, hackers and thief.**

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

In conclusion…

·This game is for everyone, who want to relax and tune out from casual life. But you have to remember that it is not real life and there are many threats.

“Second Life destroys my life and I tell myself, I have only ONE life and I better behappy with it and make the best out of it. There is no SL vs RL balancing act. YOUONLY LIVE ONCE.”

“We used to say that our only competition was real life.”

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Hackers

Hacking and hackers are the stuff of mythology, film, and often breathless headlines. From the attacks that brought down Mastercard and Visa's websites in 2010 to the Xbox Live and PlayStation outages of Christmas 2014, it sometimes feels like our systems are under permanent assault from those who would take them offline.

Hacking, as first demonstrated in 1903 by magician John Nevil Maskelyne when he hijacked a public demonstration of Marconi's telegraph, involves gaining unauthorised access to a computer or IT system and requires some skill.

While small-scale attacks, malware and botnets still do the rounds, large-scale disruptive hacks are rare. When they do happen, though, they can be spectacular.

STUXNET

Stuxnet is one of the best known names when it comes to cyber attacks, and for good reason. The worm (a self replicating, self propagating computer virus) destroyed a fifth of Iran's nuclear centrifuges in 2009, seriously hindering the country's atomic plans.

It was also propagated by an unusual means. For four years, it was thought the virus was introduced into the Natanz uranium enrichment facility, the primary target of the attack about 1,000 centrifuges were damaged, via an infected USB stick. However, researchers at Kaspersky Lab discovered in 2014 that the vector of attack was in fact the plant's supply chain.

Five organisations supplying Natanz were the initial victims of Stuxnet, including a company named NEDA, the lead supplier of the Siemens centrifuges that were the ultimate target of the worm. It's now thought that these organisations, and NEDA in particular, were the real vector of infection.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

So why wasn't the worm detected at this initial point of infection? The answer lies in what Stuxnet did.

As Ralph Langner, one of the first people to decode the worm, described it, to describe it in an interview with the New York Times, Stuxnet was "a marksman's job". Unless you were running a uranium enrichment facility, it lay dormant, with the rootkit hiding its presence. There was no way for the Stuxnet Typhoid Marys to know they were being used by the attackers. The sophistication of the Stuxnet program led many to believe it was created by a nation state and, given the target, that the US and Israel were probably involved.

NASA HACK

At the turn of the millennium, NASA and the US Department of Defense (DoD) were successfully compromised by two hackers, 15-year-old Floridian Jonathan James and 35-year-old Scot Gary McKinnon.
James was the first to have a crack at the American space agency in 1999, which he crawled into by compromising computers at the US Defense Threat Reduction Agency.
Among other things, he managed to make off with the source code for the life support systems on the International Space Station (ISS).
According to American authorities, between February 2001 and March 2002 he hacked into 97 computers, 16 belonging to NASA and 81 belonging to other parts of the DoD.
During his actions, which he claims were carried out in search of evidence of UFOs and the suppression of new energy technologies, McKinnon managed to paralyse munitions supplies to the US Naval Fleet in the Atlantic in the immediate aftermath of 9/11 by deleting weapons logs.
He is also alleged to have stolen 950 passwords and dozens of documents in the course of his actions.
As the hacks were carried out against the military, it's not been made public how exactly James and McKinnon gained access to the systems they did, but we do know what happened to the men in question.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Mt. Gox

How can millions of dollars disappear without trace? This is the question Mt. Gox, the largest Bitcoin exchange in the world, was faced with in early 2014.

On 7 February, the exchange suddenly ceased trading, saying it had discovered a "transaction malleability" bug and locked customers out of their accounts. The organisation would later blame hackers for stealing $460 million-worth of Bitcoins over the course of three-to-four years, causing a crash in the value of the cryptocurrency.

While this crisis led to the eventual bankruptcy of Mt. Gox, there was an earlier hack that foreshadowed what was to come in 2014.

On 13 June 2011, 478 Mt. Gox accounts were robbed of a total of 25,000 bitcoins (worth between $375,000 and $500,000 at the time), which were all transferred into a single account.

Mt. Gox largely blamed the victims for the theft, as the perpetrator had apparently used valid account passwords to gain access and carry out the transaction.

"As a reminder we assume no responsibility should your funds be stolen by someone using your own password," said Mt. Gox CEO Mark Karpeles, using the alias MagicalTux.

However, the 25,000 bitcoin theft was just the beginning. Towards the end of the same week, it became apparent the reason the 478 accounts were compromised using their own passwords was because a hacker had managed to access the Mt. Gox database and steal the usernames and passwords of all 60,000+ customers.

Karpeles seemed initially quite relaxed about claims the entire Mt. Gox database had been compromised, saying : "Passwords are encrypted one way. Someone cannot be selling 'user + pass' unless he has some way to revert this."

By 20 June, though, he was taking things a bit more seriously, when a huge Bitcoin sale from one of the compromised accounts caused the value of the cryptocurrency to crash to near zero. One of the defining features of the early part of the PSN hack was Sony's reticence to share information with the public. It took two days for Sony to give any kind of explanation

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

In an official announcement on the Mt. Gox site, Karpeles explained that an admin account had been compromised and the attacker responsible had used the associated permissions to "arbitrarily assign himself a large number of bitcoins, which he subsequently sold on the exchange".
In doing this, the hacker flooded Mt. Gox with more bitcoins than were actually in the exchange's wallet, bringing the value of the cryptocurrency crashing down from $17.50/btc to $0.01/btc, while also relieving another account of 2,000 bitcoins.
In the same statement, Karpeles also confirmed the loss of the Mt. Gox database, stating this was likely how the hacker gained access to the admin account that caused the crash and the one that was robbed of 2,000 bitcoins.
The damage was undone by shutting down the exchange and rolling back the transactions that had taken place during the attack, while the lost 2,000 bitcoins were refunded at Mt. Gox's own expense.

PlayStation Network

Sometimes hackers manage to pull of something so audacious it becomes part of infosec legend: the 2011 LulzSec hack of the PlayStation Network is one such case.
In mid-April 2011, users trying to log in to the PlayStation Network (PSN) were greeted with a message stating the system was "currently undergoing maintenance" or simply that "an error [had] occurred", preventing them from logging in.
On 20 April, Sony acknowledged there was a problem with "certain functions of PlayStation Network" and that it would report back with more information when it was available.
Instead, later that night, Sony shut down the network completely - an outage that would last a month.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

A short post to the PlayStation blog on 22 April from then director of corporate communications, Patrick Seybold, said simply: "An external intrusion on our system has affected [the] PlayStation Network and Qriocity (now Sony Music Unlimited) services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off ... [the] services on the evening of Wednesday, April 20th."

It would be another four days until Sony revealed the extent of what had happened, and it was huge.

Between 17 and 19 April, LulzSec hackers managed to completely breach Sony's security measures gaining access to all 77 million users' real names, postal addresses, country, email address, date of birth, PSN and/or Qriocity username and password, and security answers.

While this would have been bad enough, it was compounded by the fact that 12,700 card details, along with billing addresses and purchase history, were also taken during the hack.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Influence of social media

Social media has grown tremendously in the last few years. It has brought a lot of benefits for the people and also bad aspects for the people. Now it depends on people that the people used social media either for good aspects or bad aspects.

Advantages:

• Social Media in Development of Discussion - Social media plays a very important role in the developing of discussion.There is a lot of groups and pages related to different things. If you want to find some information about anything
• Education - Social media has a lot of benefits for the students and teachers. It is very easy to educate from others who are experts and professionals via the social media. You can follow anyone to learn from him/her and enhance your knowledge about any field.
• Helps Govt and Agencies Fight Crime - It is also one of the advantages of the social media that it helps Governments and Security Agencies to spy and catch criminals to fight crime

Disadvantages:

• Addiction – The addictive part of the social media is very bad and can disturb personal lives as well. The teenagers are the most affected by the addiction of the social media. They get involved very extensively and are eventually cut off from the society. It can also waste individual time that could have been utilized by productive tasks and activities.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

• Glamorizes Drugs and Alcohol – One of the disadvantages of the social media is that people start to follow others who are wealthy or drug addicted and share their views and videos on the web. Which eventually inspires others to follow the same and get addicted to the drugs and alcohol.

• Hacking – Personal data and privacy can easily be hacked and shared on the Internet. Which can make financial losses and loss to personal life. Similarly, identity theft is another issue that can give financial losses to anyone by hacking their personal accounts.

Taking everything into account, influence of internet and social media is rising dramatically due to the popularity and daily opreation. Although using social media can be addictive and glamorize bad habits and lifestyle, it is also a good platform where you can gain knowledge and interract with people from simillar fields.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Cyberbullying

Add a little bit of body textCyberbullying is defined as the sending or posting of damaging or cruel text or images using the
internet mostly through social media or other digital communication services. It is especially popular amongst the younger generation. Also, there are different types of cyberbullying with different ways to commit such an act:

- Flaming: Online fights using electronic messages with angry and vulgar language.
- Harassment and stalking: Repeatedly sending cruel, vicious and/or threatening messages to the victim.
- Denigration: Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.
- Impersonation: Breaking into someone's email account and using it to send vicious or embarrassing material to others.
- Outing and trickery: Engaging someone in instant messaging, tricking him or her into revealing sensitive information, and forwarding that information to others.
- Exclusion: Intentionally excluding someone from and online group.
- Cyberstalking: Repeated, intense harassment and denigration that includes threats or creates
significant fear.

This type of bullying (the same as real life bullying) causes significant emotional and psychological
distress. In fact, just like any other victim of bullying, cyberbullied kids experience anxiety, fear,
depression, and low self-esteem. They also may experience physical symptoms, and struggle academically. Many even experience even unique negative consequences.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Future of the Internet and AI

Nowadays the Internet has a significant impact on daily life of people. Internet has positive and
negative sides – it provides a possibility to get newest information, communicate with people from all around the world and do a lot of things the way faster and easier. However, we are becoming addicted to the Internet. Can we imagine what the internet and artificial intelligence could offer in the future?

Perspectives of the future depend on the way how people will use technologies connecting them to the Internet. If artificial intelligence is connected to the internet, computer will be attached to an endless database. In that case, it will be possible to process millions of operations per second. Therefore, fast and uncontrollable development of technologies would be capable. Computer will be able to calculate the duration of the Earth's lifetime. These days mankind controls the amount of animal's species on the Earth. Even so, artificial intelligence could control the life of humans. As a consequence, people would be wiped from the surface of the Earth. No one can protect us from powerful computer which is connected to the web. World conflicts as well as extinction of mankind would be outcome of strong AI prototype. Finally, robots would master the Earth. Today we have plenty of science-fiction movies like "Blade Runner", "Terminator" and "Ex Machine", where we can see how technologies can affect us. Overtime, it might happen in reality.

Nevertheless, robots are not capable to replace the emotions of humans. As long as people apply technologies wisely, the human race is safe.

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Posters

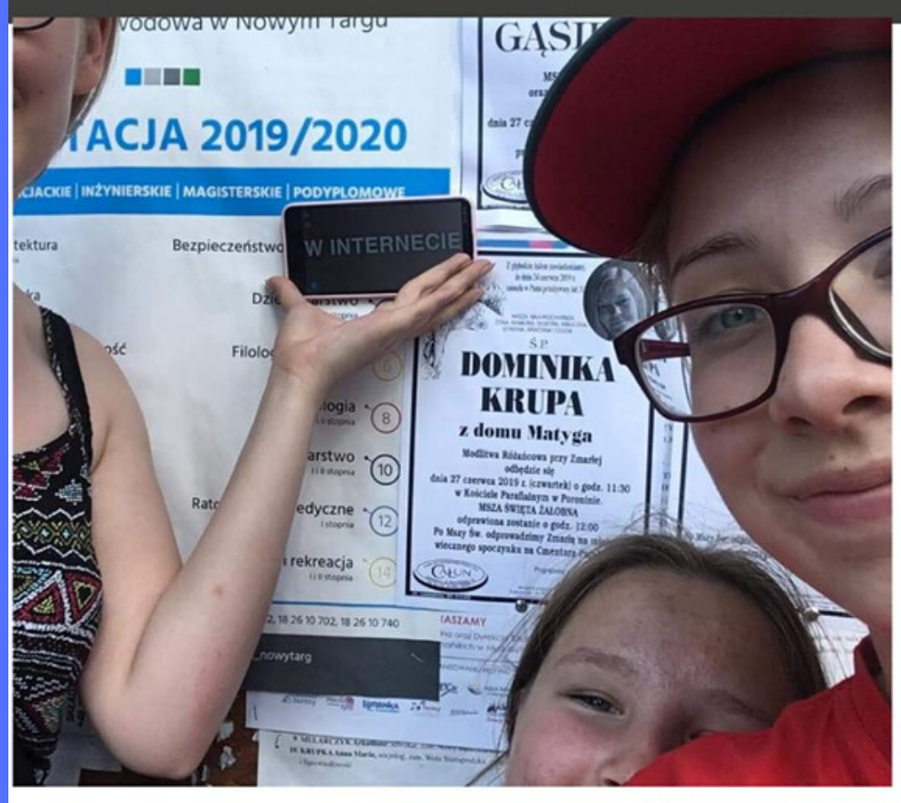
BE CAREFUL ON THE WEB

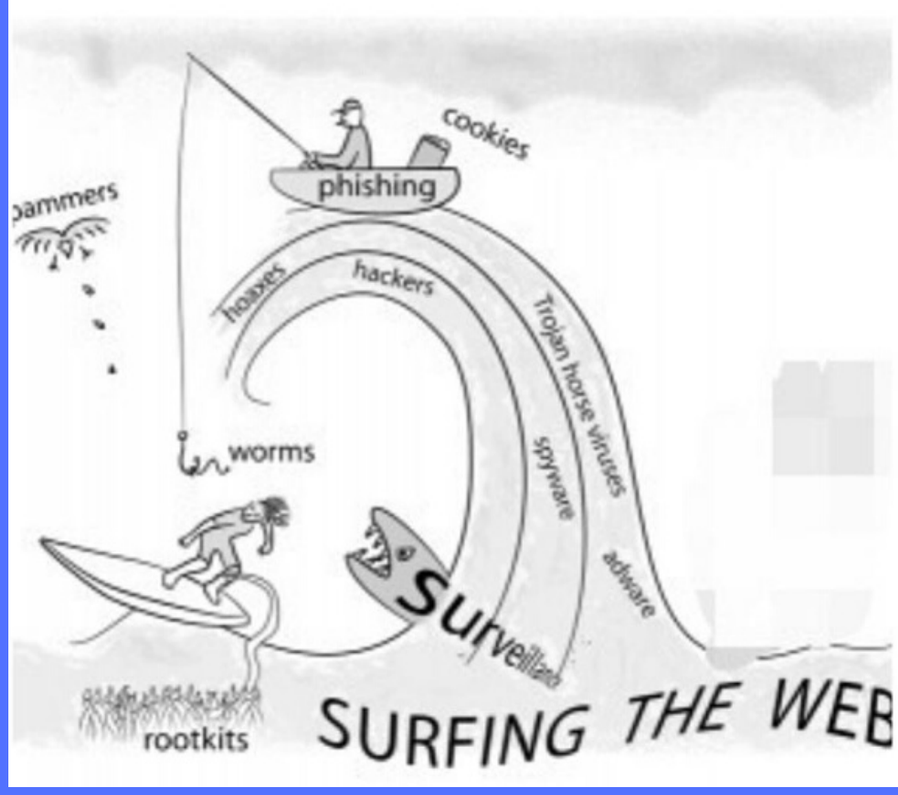
CAREFUL WITH THE WEB, IT COULD HAUNT YOU LATER

Did you know....

71% of have established online profiles on social networking sites

Nearly half have public viewable by anyone.





Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

GUIDELINES FOR INTERNET SAFETY

Be aware of the malware

Catfish is your last wish

Tight privacy is a mighty key

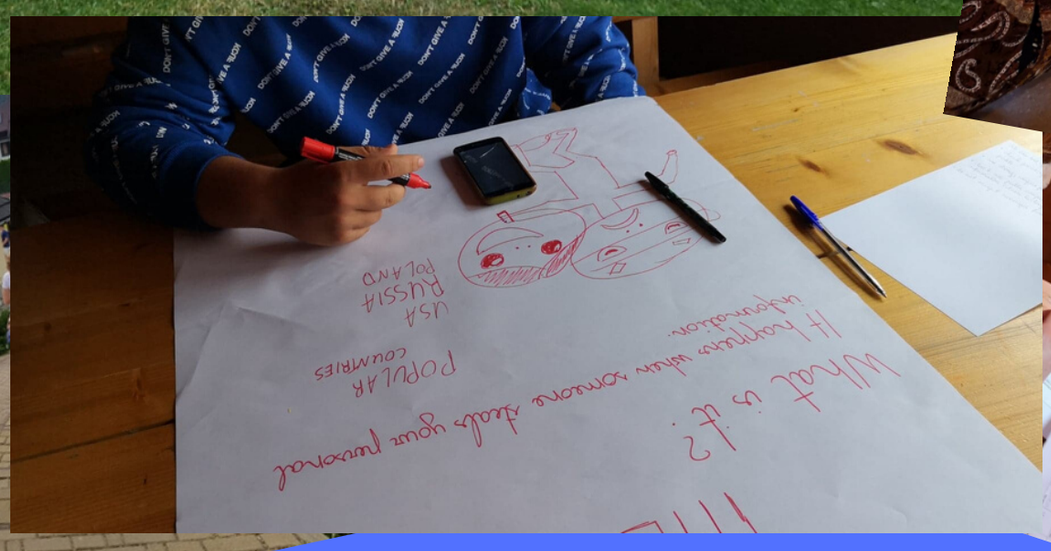
There’s a vulnerability in every facility

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Our gallery from the first Youth Exchange

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Our gallery from the second Youth Exchange



Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme

Erasmus+

Project Partners

Inovacijų biuras

Project "Be carefull of the Web" no. 2018-3-PL01-KA105-061189
funded by Erasmus+ Programme