

Scenario 1

Technology and IT (e.g. materials, processes, production organization, IT)

BRinging STEM into Active aglNg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Partner name: Foro de Formación y Ediciones



This material is created in the framework of BRAIN project “BringING STEM into Active AgING” (GRANT AGREEMENT 2020-1-PL01-KA204-081805. This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Leakage of personal data, creating strong passwords, password organizers

BBringing STEM into Active agING – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Partner name: Foro de Formación y Ediciones



This material is created in the framework of BRAIN project “BringING STEM into Active AgING” (GRANT AGREEMENT 2020-1-PL01-KA204-081805. This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Ice Breaker

Let us get into a circle. Then start out by saying your name and an IT related word that begins with the same letter. E.g. Adam Application, Bartek Banner, Celine Cookies, Darek Domain, etc....

Then the next person does theirs, plus yours. Then the third person does theirs, the second's and the first's name and an IT related word. It then moves on down the line, so that the last person has to do everyone with in the group. Different variations of this can be played but it is great for getting the group to know one another and the names.



Introduction

The internet has become a determining factor for the development of today's society. It has been used as the main means for the interaction of people and computers, exchanging information and promoting the rapid transmission of experiences and knowledge regardless of geographic location.



Introduction



From its beginnings in the 1960s to the present day, the Internet has been a fundamental ingredient for technological development, education, communications, medicine, science, art and practically all disciplines and professions. In a globalized world. Although initially it was intended for military use, its benefits were radically extended to practically any field.

Introduction



Commerce is another space in which the internet has managed to have a positive impact, both for the seller and for the buyer. Large supermarkets and chain stores, in addition to having their points of sale, have developed platforms for online sales, managing to lower some costs such as sales staff and locations, for example. Electronic commerce allows companies to cross borders without the need to be physically in one place. This has resulted in business efficiency and opened up new avenues of trade.

Introduction

In addition, electronic commerce is no longer exclusive to the big brands. The versatility of the business has allowed small and medium-sized companies to also venture into the business, and social networks have made an interesting contribution to this dynamic.



Introduction



The internet is therefore today a global means of communication that allows us to interact in different spaces. From communicating through a video call or a chat with another person thousands of kilometers away, accessing quality education in institutes and universities in different parts of the world, buying products or services online, reading newspapers, magazines or books, listen to music, watch movies, or interact on social networks. This, to mention just a few of the many possibilities it offers us.

Introduction

It is in our hands to make a rational and objective use of a tool as powerful as we would like it to be.



The way in which the internet has evolved since its invention is fantastic and it has let us see that it will continue to evolve so fast that it will not cease to amaze us.

Fake news - that is, searching the Internet, verifying information provided by the media. Fake News Flipchart

Materials

telephones/tablets/laptops with Internet access, overhead projector, pens, markers, flipchart, ticky notes, A4 sheets of paper

Directions

The presenter writes down the term "FAKE NEWS" in the middle of the flipchart. Distribute 3 Post-it notes to the participants and ask them to write down their associations with the term and glue them to the flipchart. Read out the written associations, grouping them together if possible. Discuss each association and compare it with the definition of fake news (appendix below).

Appendix

The term "Fake news"

Fake news is "untrue, false news, usually spread by tabloids in order to cause sensation or to defame someone (usually a politician)". The Cambridge Dictionary says it is (translated) "false stories that appear to be news, disseminated on the Internet or through other media, usually created to influence political views or as a joke."



Fake news - that is, searching the Internet, verifying information provided by the media. Fake News Flipchart

The term "fake news" is a neologism and is difficult to place in a definitional framework. It denotes media news that is neither true nor false at the same time and is based on disinformation, often including true parts. Fake news is usually based on disinformation or a joke, often containing true elements. Fake news can pretend to be real information, articles, social media posts, memes, etc. They can be created with a variety of intentions, from deception, to tools of propaganda, to create sensationalism, to a joke.

Fake news is "a manipulation of facts, eagerly used by journalists whose aim, while preparing a publication, is to arouse as much interest in the topic as possible, and not its conformity with reality.

The Internet is currently the most popular source of communication. However, the content published on it should be approached with caution. The IAB study "Disinformation in the Web. Analysis of the credibility of information channels" shows that social media are the leader in spreading fake news. In second place are internet portals.

Types of fake news:

total untruth - the information provided is fabricated, contradictory,

the truth is disputable - facts are presented selectively or in the right context, which results in misleading the recipient,

quote manipulation - the statement is placed in the appropriate context or sentences or their fragments are removed, which changes the sense of the statement, and consequently supports the specific thesis.



Fake news - that is, searching the Internet, verifying information provided by the media.

Fake News Videos

Materials

telephones/tablets/laptops with Internet access, overhead projector, pens, markers, flipchart, ticky notes, A4 sheets of paper

Directions

Using an overhead projector, the presenter shows short films on what fake news is and how to recognize it. How false news can spread - Noah Tavlin (English, subtitles available in other languages)

https://www.youtube.com/watch?v=cSKGa_7XJkg

How to choose your news - Damon Brown (English, subtitles available in other languages)

<https://www.youtube.com/watch?v=q-Y-z6HmRgl>

Introducing to the group the elements thanks to which one can recognize fake news, distinguish it from real information (appendix below).

Appendix

INTERPRETATION OF SOURCE MATERIAL:

- pay attention to emotional language, brutal descriptions
- be aware of your own bias
- ask questions about the material (who is the author? is the message consistent? do other sources confirm the information? etc.)



Fake news - that is, searching the Internet, verifying information provided by the media.

Fake News Videos

- pay attention to whether the pictures used are set in a real context
- verify the credibility of the website - is the URL correct and leads to the correct, genuine website
- check the date and timeliness of the information
- verify the author - if he/she is credible, what are his/her goals and intentions, if he/she has already published other materials online
- check if images do not look strange or have not been manipulated - this can be done e.g. by using the reverse image search option available in search engines

FAKE NEWS - GENERAL RULES:

They are dominated by images/photos and short text.

The message is strongly emotionally charged: it uses hate speech, shows violent, moving scenes and images.

Often pretends to be first-hand.

They use generally known truths and beliefs.

They often show half-truths, misrepresent facts in such a way that it is impossible to know where verified information begins and where it ends. They are based on the assumption that a partial truth confirms the truth of the whole.

Sometimes they describe true events but change their context.

They almost always include pictures or videos to help increase coverage quickly.

They don't communicate that the information given may not be certain.

They avoid nuance and different points of view.

Time for Question...

What can you tell me about online privacy?



Time for Answer...

The definition of online privacy is the level of privacy protection an individual has while connected to the Internet. It covers the amount of online security available for personal and financial data, communications, and preferences. Internet privacy is important because it gives you control over your identity and personal information. Without that control, anyone with the intention and means can manipulate your identity to serve their goals, whether it is selling you a more expensive vacation or stealing your savings.



The importance of passwords

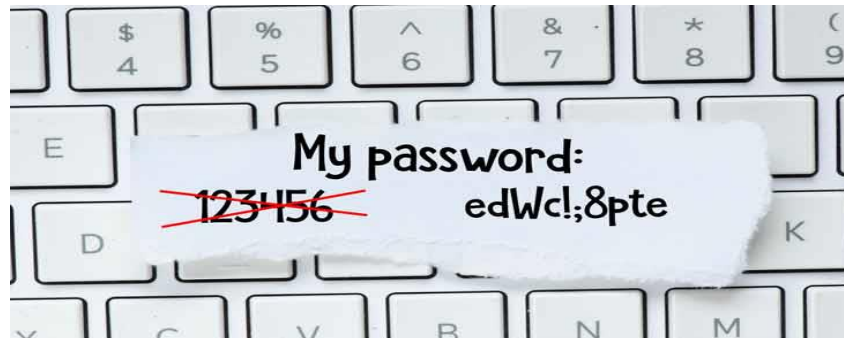
Passwords are the key that opens the door to the use of all our services. If our passwords are exposed, cybercriminals could be able to use them to enter them and impersonate us, make payments in our name, change or access other types of information or other people, among other things, so it is advisable to take a series of measures for our protection.



The importance of passwords

A password must be strong, with a minimum of 8 characters and be composed of:

- Uppercase (A, B, C...)
- Numbers (1, 2, 3...)
- Lowercase (a, b, c...)
- Special characters (\$, &, #...)



It is important to use passwords that are not easy to guess. For example: "123456789", "qwerty", "aaaaa", proper names, birthdays, etc...

The importance of passwords



Passwords should not be shared with anyone, a password must belong exclusively to the user who creates it and only be used by the user. Sharing it will make us vulnerable and even more so if the way in which we share it is a messaging network such as (WhatsApp, Telegram, Facebook), since the information is stored on the servers of these services.

The importance of passwords

Try to avoid using the same password for all services at all costs, since if a cybercriminal gets hold of that password, they will be able to access all of them.



The importance of passwords



Change passwords periodically and not a permanent one forever. A good way to remember when we should change our passwords is to keep in mind the seasons of the year. A password change for each station, so it would always be updated every 3 months.

The importance of passwords

As advice to all the large number of passwords that would have to be managed in case of having one per service, there are password managers that make life easier when it comes to remembering them all.



2-step authentication

Sometimes, having a password is not enough, no matter how strong it may be, or after following all the previous steps.

Cybercriminals could get hold of them through different techniques such as "phishing" or some viruses designed for this that we will see later.



2-step authentication

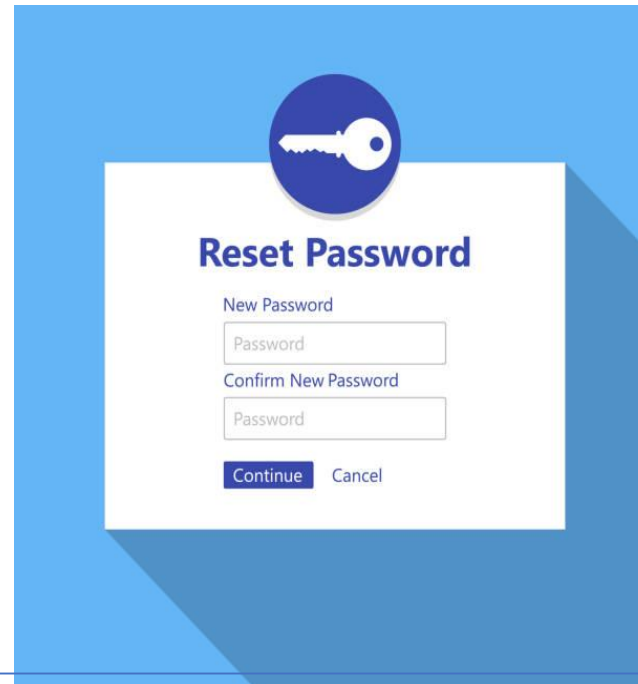


That is why many services already offer two-step authentication. With this method we will use our service password in the normal way and then it will ask us to add a second code.

The most common way to receive this code is to receive it as an SMS to our Smartphone, although it can also be a phone call through a machine or by having a service app that actively changes the codes every 5 minutes.

2-step authentication

Clearly the service has had to be previously configured to link our smartphone to it and receive the codes. In this way, even if the cybercriminal obtains your password, they will not be able to access the service since they will need this second code to enter.

A screenshot of a "Reset Password" web form. At the top is a blue circular icon containing a white key. Below it, the title "Reset Password" is displayed in bold blue text. The form contains two input fields: "New Password" and "Confirm New Password", both with "Password" as placeholder text. At the bottom are two buttons: a blue "Continue" button and a grey "Cancel" button. The entire form is set against a light blue background with a subtle shadow effect.

If at any time you find yourself with an attempt to access your account because you have received the double authentication code and it was not you, you should consider changing the password as it is very likely that it is no longer a secure key.

Time for Question...

What is Spying / snooping?



Time for Answer...

When you are online, you are spied by a number of trackers for various purposes. Trackers keep a record of your search history and track all your online activities through various means. This provides them a clear picture of who you are and your interests, which is a breach of online privacy policy and makes you a public property. Most of the time, this tracking is for advertisement purposes only and it allows advertisers to show ads according to your taste and interests. But sometimes this information is used by cybercriminals to carry out unauthorized and illegal activities risking your online existence.



Personal data

Before providing your personal data, you must analyze who is asking you for it? what do you need this information for?

The information that you will have to provide, for example, to contract a bank account, is not the same as that of subscribing to an online shopping website. In the first case, the required information will be substantially extensive, but in the second, the name, surname, delivery address, billing data and payment method would be sufficient.



If someone requests your personal data, you must inform yourself about the purpose, what they are going to use them for, as well as their treatment and how long they are going to keep your data.

It is useful to know how to exercise your rights (Access, Rectification, Opposition, Limitation of treatment and Portability).

Phishing



Phishing is the identity theft of a service or company to try to scam people. For example, you could receive an email asking you to update your bank details because your credit card is about to expire. In this email comes a link to access this service. When opening it, a web page appears that is a copy of the original, the user updates the data of his bank account and that is when he has fallen for the deception.

Phishing

Tips to avoid being a victim

1. Be wary of emails that appear to be banking entities or well-known services with messages of the type:
 - a. Technical problems of the entity
 - b. Security problems in the user account.
 - c. Security recommendations to avoid fraud.
 - d. Changes in the entity's security policy
 - e. Promotion of new products
 - f. Discount vouchers, prizes or gifts
 - g. Imminent cessation or deactivation of the service.



Phishing



2. Be suspicious if there are grammatical errors in the text.
3. If you receive anonymous communications addressed to "Dear customer" or "User notification" it is an indication that should alert you.
4. If the message forces you to make a decision in a few hours, that's a bad sign. It directly contrasts whether the urgency is real or not with the service through other channels.
5. Check that the link text matches the address it points to.
6. A reputable service will use its own domains for corporate email addresses. If you receive the communication from a mailbox type @gmail.com or @hotmail.com, it is not a good sign.

Phishing

What you should do if we detect a case of phishing

1. Do not reply to these emails under any circumstances. If you have doubts, ask directly to the company or service that it represents.
2. Do not access the links provided in the message or download any attached document.
3. Delete the message and alert your contacts about the fraud.



Time for Question...

What do you know about Information mishandling?



Time for Answer...

There are various sites on the internet that need your personal information to get access to their services. These sites often store cookies and save your personal information and later use it for various purposes. Most of the time this information is not encrypted and can be accessed by anyone. This mishandling of personal information may lead to serious consequences. The modern trend of e-banking and e-business portals have multiplied the risks associated with online privacy. By sharing your bank details and crucial files on the internet, you are paving ways for burglars and making yourself vulnerable to cybercriminals.



Leakage of personal data, creating strong passwords, password organizers

Game: Two truths and one lie

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

Game Two truths and one lie. The participants are given three statements. Two will be true, one will be a lie. The participants need to identify the lie.

Appendix

The participants are given three statements. Two will be true, one will be a lie. The participants need to identify the lie. All the statements will be related to Internet topics.

Online Shopping:

1. Credit card is one of the most dangerous ways to pay for goods online
2. You should never enter your payment details on a page unless there is an S after HTTP
3. If you don't have a credit or debit card, PayPal is a good alternative to pay for goods online

Malware:

1. Malware is a type of computer virus
2. A computer worm frequently exploits computers running out-dated software
3. An important step to protect yourself from ransomware is regular backups

Leakage of personal data, creating strong passwords, password organizers

Game: Two truths and one lie

Phishing:

1. If an email addresses you as 'customer', you should be especially wary of it
2. A phishing scam that knows personal details pertinent to the recipient is called a spear-phishing attack
3. Clicking a link in an email is okay if the email is from a bank you have an account with

Social Media privacy:

1. The only recommended default privacy level is friends and family ONLY
2. Installing social media apps (Facebook, Instagram, Twitter...) can give total strangers access to certain information about you
3. If I block someone on Facebook or Twitter, that person has no way of seeing anything I do with or post on my account

Facebook scam:

1. Adding a stranger on Facebook gives them access to my computer
2. Adding a stranger on Facebook could put my friends at risk
3. Adding a stranger on Facebook could lead to identity theft

Leakage of personal data, creating strong passwords, password organizers

Game: Two truths and one lie

Email scams:

1. Advance fee email scams rely on tricking a victim to send money on the promise of a much bigger return
2. An email attachment that contains a Word Document can still be dangerous to open
3. The best course of action if I get a 'Nigerian Prince' email scam is to reply and tell them to stop emailing me

Ransomware

1. If ransomware infects my computer, a reliable and reputable anti-virus program can remove it.
2. Anti-virus can reverse the effects of ransomware
3. Ransomware is one of the most prolific online threats of 2017 and 2018

After these examples, participants will have to think up at least one more each. They will then try to find out which statement is incorrect.

Leakage of personal data, creating strong passwords, password organizers

Game: Two truths and one lie

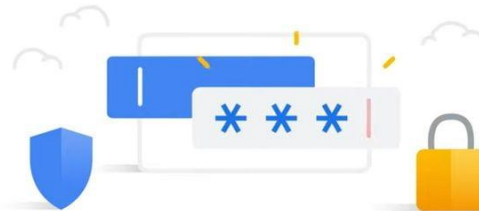
Answers:

1
3
3
1
1
3
2

Password Managers

Having a free version of a great password manager
is always better than having none at all.

Password Manager



Password Managers

1Password: great family option → https://cnews.link/get-1password_7/

=====

Free plan cons:

- ✓ Checks for compromised passwords
- ✓ 24/7 email support
- ✓ Unlimited users for one account
- ✓ Local storage option



Free plan limitations:

- ✗ No live chat support
- ✗ No one-click password updates

Password Managers

NordPass: most versatile password manager → https://cnews.link/get-nordpass_46/

=====

Free plan pros:

- ✓ Next-gen encryption
- ✓ Unlimited password vault storage
- ✓ Multi-factor authentication
- ✓ Easy vault transfers
- ✓ Live chat customer support

Free plan limitations:

- ✗ Most features are behind a paywall
- ✗ Lacks add-ons for more browsers



Password Managers

Dashlane: a secure and streamlined experience → https://cnews.link/get-dashlane_39/

=====

Free plan:

- ✓ Password sharing with 5 users
- ✓ Superb reputation
- ✓ 2FA support
- ✓ Store up to 50 passwords

Free plan limitations:

- ✗ The maximum amount of stored passwords is 50
- ✗ iOS version is lacking
- ✗ Limits user to one device



Password Managers

Keeper: outstanding password management tool → https://cnews.link/get-keeper_10/

=====

Free plan cons:

- ✓ Great compatibility
- ✓ Multiple 2FA options
- ✓ Private messaging app



Free plan limitations:

- ✗ Few export options

Password Managers

RoboForm → https://cnews.link/get-roboform_10/

=====

Free plan cons:

- ✓ Unlimited password vault storage
- ✓ Convenient updating of weaker passwords
- ✓ Password sharing via email
- ✓ Dark web monitoring

Free plan limitations:

- ✗ Could be more user-friendly
- ✗ Live chat only for paid users



Time for Question...

Can you tell me what identity theft is and some of the ways in which it is carried out? (phishing, malware, pharming, discarded computers and phones...)



Time for Answer...

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.



Leakage of personal data, creating strong passwords, password organizers

Game: Who are you talking to?

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

This game is supposed to simulate when you talk to someone on internet and you don't really know who is on the other side of the screen, whether they are telling the truth or not, or if they are pretending to be someone else for a hidden purpose.

Each participant is assigned a character and others have to find out who they are. But some of them will not match the truth. Those who do not have a character in pairs or groups (depending on the participants) have to guess through questions who is the person they are talking to (the one who has the assigned role). It is designed for a group of 15 people, where 5 have characters and 10 in pairs will try to find out who the character of the other 5 is and if he/she is real or not. The game will be played in two groups of 15 participants each.

The people with assigned characters have to answer the questions as if they were the characters. The pairs will know that it is possible that some of the characters are not who they say they are. The 5 pairs will ask questions to each other for a few minutes and rotate. After finishing with everyone, each pair has to say who they think each character is and if they really are who they say they are.

Leakage of personal data, creating strong passwords, password organizers

Game: Who are you talking to?

Character 1:

20-year-old boy. He likes football, going out with his friends and going to concerts.

Character 2:

25-year-old girl. She plays in a rugby team and likes mountain sports. She likes animals and has a dog.

Character 3: (Fake character)

Answers as: 18-year-old girl. Biology participant. She likes nature and plants. She is a fan of Rosalia.

Actually he is: 39 years old man.

Character 4: (Fake character)

Answers as: 23 year old boy. He likes rock music and surfing. Usually plays video games.

Actually he is: 47 year old man.

Character 5:

27-year-old boy. He plays paddle tennis. He likes animals and has two cats. He works as a graphic designer.



Leakage of personal data, creating strong passwords, password organizers

Game: Who are you talking to?

What's happening?

This game is supposed to simulate when you talk to someone on internet and you don't really know who is on the other side of the screen, whether they are telling the truth or not, or if they are pretending to be someone else for a hidden purpose.

Each participant is assigned a character and others have to find out who they are. But some of them will not match the truth.

The people with assigned characters have to answer the questions as if they were the characters.

Scenario 2

Technology and IT (e.g. materials, processes, production organization, IT)

BBringing STEM into Active agING – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Partner name: Foro de Formación y Ediciones



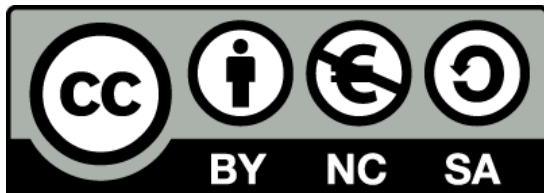
This material is created in the framework of BRAIN project “BringING STEM into Active AgING” (GRANT AGREEMENT 2020-1-PL01-KA204-081805. This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Problems with online purchases and money transfers

BRinging STEM into Active aglNg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Partner name: Foro de Formación y Ediciones



This material is created in the framework of BRAIN project “BringING STEM into Active AgING” (GRANT AGREEMENT 2020-1-PL01-KA204-081805. This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Ice Breaker

The group forms a circle. Participants throw a ball to each other. Everyone gives an association to the previous word spoken by the person from whom they receive the ball. The activity is repeated.

What's happening?

Icebreakers are fun activities to help people get to know one another. Instructors can use them to help acquaint participants with course content and expectations. Icebreakers can also be designed to help warm up online learning spaces and orient participants to the online environment.



Mobile payments

Digital wallets is a medium to store multiple physical credit or debit cards.

Banking App which can be used for authentication purposes as required when making transactions or to access banking services. Usually, every bank have it own application.

Benefits of mobiles payments

Touch ID in the form of fingerprint scan or PIN input makes them more secure than physical credit or debit cards,

Elimination of a physical wallet

People are unable to see what card you have (Some cards are provided for clients with low limits of credit score. Some people feel shame showing it around other people.)

Act as an easier third party payment provider when paying on e-commerce websites

Time for Question...

What are cookies? What are they for?



Time for Answer...

Cookies are small pieces of text that the websites you visit send to your browser. They allow websites to remember information about your visit, which can make it easier to revisit sites and make them more useful to you. They are temporary files that can last for a shorter or longer period of time. We can configure them, use tools to block them, delete them whenever we want... The problem can come mainly when they collect personal data without notifying the user.



Problems with online, card purchases and money transfers.

Safe online shopping

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

Participants will be sitting in the circle. Trainer on the flip chart will be writing giving guiding questions to the participants helping them to come up with rules to shop safely online (appendix below).

Appendix

- use familiar website
- use website safety evaluation tool for the new websites
- look for the lock
- do not share your sensitive data with everybody
- Use private Wi-Fi
- Create strong passwords
- Do not buy with card in public places

Digital wallets

•Examples:

•Apple Pay, Google Pay, and Samsung Pay are probably three of the most popular digital wallets, but there are quite a few others. Some other popular digital wallets include PayPal and Venmo, both of which are uniquely social by allowing you to easily send money to retailers and friends.

Problems with online, card purchases and money transfers.

Dangers of using money in digital space

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

The presenter writes down the term "Dangers of using money in digital space" in the middle of the flipchart. Distribute Post-it sticky notes (different colors) to the participants and ask them to write down their associations with the term and glue them to the flipchart. Read out the written associations, grouping them together if possible. Discuss each association and try to get to know the dangers online related to money (appendix below).

Appendix

Dangers of using money in digital space

1. You card information can be stolen (IBAN, CVC, expiration date)

Your personal information can stolen (Full name, ID code, date of birth, phone number, passwords)

ARE DIGITAL WALLET SAFE?

Digital wallets are actually more secure than physical cards, because mobile payments are heavily encrypted and tokenized, meaning that none of your actual card or account numbers are stored within the digital wallet.

Digital wallets go a step further by also adding in tokenization, which takes that sensitive encrypted data and replaces it with a non-sensitive digital equivalent known as a token. These unique tokens are randomly generated every time a user makes a payment and only the merchant's payment gateway can match this token to accept the payment.

Not only is your information more secure thanks to that technology, but also through user verification. This added layer of security is usually done by fingerprint, facial recognition or PIN.

Apple and google pay similarity

Both systems are using NFC technology

Both Google Pay and Apple Pay can make online purchases straight from an app or website, automatically handling the entire checkout process with pre-filled defaults and only requiring PIN or Touch ID verification to complete the transaction.

Both are more secure than physical debit and credit cards, because system does not reveal the user's card details to the vendor.

Apple and google pay Differences

Apple pay allows authentication with Touch ID or Face ID, but is compatible only with new hardware gadgets.

Google, on the other hand, opts for a more traditional PIN-based authentication system. This allows it to work on older hardware.

You can add any credit or debit card to google pay. In apple pay you can add only credit or debit cards that Apple company have contacts with banks issuing physical cards.

Time for Question...

Do you know what is cloud data?



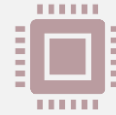
Time for Answer...

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure.





Google security? How it works?



1. User's card details are provided only once, during the initial setup to Google servers. (Google stores your card details on its servers)



2. Google saves your card details on its servers.



3. Virtual card is issued on your device with encryption of sensitive data.



4. When paying the vendor never sees your real card data, which is protected with google servers.

Apple security? How it works?



- Apple uses tokenization system.
Steps;
- When your card details are provided to the device, it contacts the issuing bank directly. (Apple does not store your card details)
- When card is confirmed with bank receives a device- and card-specific (related) token called the Device Account Number (DAN), which is stored on a secure chip on the device.
- The DAN structurally resembles a credit card number and is passed on to the merchant when any payment is made before getting authorized by the bank.
- Apple pay explained in details:
<https://www.youtube.com/watch?v=mt5FEvoEHEk>

WORKS?

Crypto wallets

Having a secure cryptocurrency wallet functions much like a regular wallet except that the currencies and wallet contents can be hacked through digital means. Additionally, having a wallet can allow users to perform various transactions while keeping an eye on their balance.

Some online banks like Revolut, Wirex, Cryptopay etc. allow to withdraw crypto coins from ATM in Euros/Dollar for free to a certain limit.



Types of crypto wallets

Software wallets

Software wallets are hot wallets as they're often connected to the Internet. These are wallets that run on a specific program that allows easy access. Some examples of software wallets include:

- Desktop wallets
- Mobile wallets
- Online wallets



Hardware wallets

Hardware wallets differ from software wallets in a sense that they store a user's private keys in a hardware device such as a flash drive. Their main purpose is to store your data offline to avoid invasion of privacy. Their main purpose is to store your data offline to avoid invasion of privacy.



Paper wallets

These types of wallets include a particular software that can be used to generate your keys and print them. Their other functions include transferring your funds to the address and moving your assets to your desktop wallet. To do the latter, users will need to manually enter their keys or scan the code included in the wallet.



Time for Question...

Could someone tell me what cybersecurity is?



Time for Answer...

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.



Advantages of different Types of crypto wallets

Hot/online/software wallets

- Spending purposes;
- Not willing to pay for a wallet.



Cold/offline/Hardware wallets

- Investing purposes;
- If you are storing more crypto currencies, then you are using.



Problems with online, card purchases and money transfers.

Scam in online shopping - videos

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

WEBSITE CREDIBILITY ELEMENTS

How to spot and avoid a scam website (English):

https://www.youtube.com/watch?v=3oEI0FCnI_Y

Tips for shopping online safely (English):

<https://www.youtube.com/watch?v=cWcNQgPiqhc>

Steps:

1. Before playing the videos above participants are asked to follow them and note not all credibility elements
 2. After watching the videos participants sitting in the circle are asked to write elements on how to check website credibility on the flip chart.
 3. Every writing is discussed right away by the writing participant and trainer (appendix below).
-

Problems with online, card purchases and money transfers.

Scam in online shopping – videos

Appendix

How to check website credibility:

Paid ads - some scammers use google paid ads to appear at the top of the google search.

Positive fake user reviews - fake websites create positive reviews to increase credibility.
positively fake user reviews.

Fake URL - some fake websites use letters from different Alphabet to mimic legitabule websites.

PadLock and HTTPS - show that the data you will have in the website is encrypted. (Third parties can not see your passwords, emails etc.)

Certificate - check website certificate expiry date and who issued it.

Company address. copyrights and contacts - company address is not found on google maps or is in a strange place (forest, desert etc.)

Copyrights, operation/working statute - should be up to date.

Fake emails - better enter links from your browser then from the emails, because it can consist spyware data to collect sensitive data.

Debit card

Debit cards are **issued by your bank and work as a combination ATM card and credit card**. However, unlike a credit card, a debit card links directly to your bank account, using the money you have on deposit to pay for your purchase or make your ATM withdrawal digitally.



Debit Cards

Pros

- Prevent debt
- No annual fees
- Good for smaller purchase
- Easy to get

Cons

- Have limited funds
- Have overdraft fees
- Complicated for big-ticket items

Time for Question...

Does anyone know how to create a strong password?



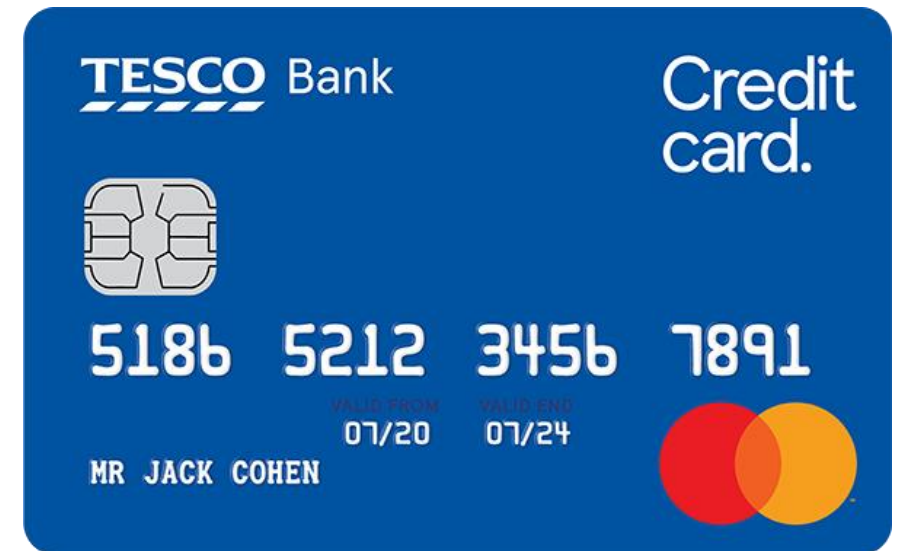
Time for Answer...

The main keys to creating a strong password are that it should be at least 12 characters long, mixing upper and lower case letters, numbers and a symbol. It is also necessary to use different passwords for each site and change them from time to time.



Credit cards

Credit cards offer you a line of credit that can be used **to make purchases, balance transfers and/or cash advances** and requiring that you pay back the loan amount in the future. When using a credit card, you will need to make at least the minimum payment every month by the due date on the balance.



Credit Cards

Pros

- Time to notice errors
- Can build credit
- Offer rewards
- Have high limits

Cons

- Can lose not a lot of money
- Can hurt credit
- Potential for overspending

Time for Question...

What is a VPN?

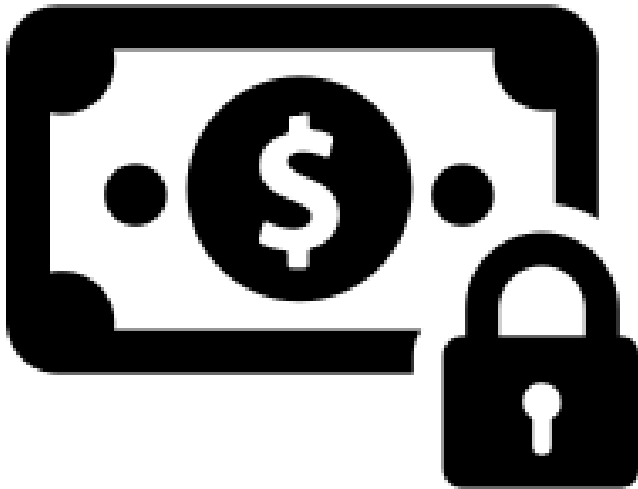


Time for Answer...

VPN stands for "virtual private network" — a service that helps you stay private online. A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks



How To Stay Safe Using Your Debit or credit Card Online



Look for the lock: Make sure you're [shopping on a secure website](#), especially when it's time to enter your card number. Look for the locked padlock icon in your browser and pay attention to any security warnings that pop up.

Monitor your account: It's always a good idea to keep tabs on your money, and it's especially important if you're sharing account information online. Check your accounts regularly: once per month at a bare minimum, though more often is better. And set up alerts in your account so you know when money goes out.

Use secure connections: Mobile devices and free Wi-Fi make it easy to get things done. But you never know [how secure a public hotspot is](#). If you're going to access financial accounts or punch in card numbers, save those tasks for when you're at home or work and know your traffic is safe.

Use Familiar Websites

- Start at a trusted site. Search results can be rigged to lead you astray, especially when you drift past the first few pages of links. If you know the site, chances are it's less likely to be a rip-off. We all know Amazon.com carries everything under the sun; likewise, just about every major retail outlet has an online store, from Target to Best Buy to Home Depot. Beware of misspellings or sites using a different top-level domain (.net instead of .com, for example)—those are the oldest tricks in the book. Yes, sales on these sites might look enticing, but that's how they trick you into giving up your info.

Time for Question...

Do you know how users are tracked in search engines? (search history, cookies, IP addresses, click-through history)



Time for Answer...

A search engine can track you across websites if the websites you visit contain the search engine's own tracking scripts as part of the page. What you search for leave a trail of information about you. This information reveals what you're interested in, what you're curious about, even what you think about those things.



Look for the Lock



- Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least.
- You'll know if the site has SSL because the URL for the site will start with HTTPS—instead of just HTTP. An icon of a locked padlock will appear, typically to the left of the URL in the address bar or the status bar down below; it depends on your browser.
- HTTPS is standard now even on non-shopping sites, enough that Google Chrome flags any page without the extra S as "not secure." So a site without it should stand out even more.

Social media - secure online image and information management

Our online safety and protection of our privacy

Materials

Laptop with internet access for the presenter, overhead projector, pens, markers, flipchart, sticky notes, A4 sheets of paper, tennis ball.

Directions

The presenter divides the participants into groups of 4-5 people and asks them to think about and write on cards answers to the question: what can we do to take care of Our safety online and protect our privacy? He then asks representatives of the groups to read the answers and write them down on the board/flipchart. After writing down all the answers, the presenter asks the participants to choose the rule that seems most important to them. Volunteers tell the other participants why they chose it. Please see below:

Furthermore: Summary by the instructor of the class, discussion about the impact of social media on Us, the opportunities and risks of using social media in the wrong way, what we can do something to increase our safety.

Joint viewing of the whole or parts of the You Tube video "The truth about social media"

<https://www.youtube.com/watch?v=DU3655oQexw>

Social media - secure online image and information management

Our online safety and protection of our privacy

Appendix

- If you are not sure who you are talking to, do not give out any information about yourself.
- Don't reveal your passwords to others. Arrange ones that will be difficult to guess (it can't be your date of birth or name!). The password should contain no less than 8 characters, including numbers and capital letters. Use different passwords on different services.
- Do not allow your browser to remember passwords for email and services you use. Log out when you are done.
- If you use social networks, make sure you have the right privacy settings. The less information you share with outsiders, the better.
- On discussion forums or blogs, use a nickname (pseudonym), not your name. Avoid publishing information about yourself online.
- Don't use the ability to automatically "tag yourself" where you are.
- Pay attention to the messages that appear when downloading games and applications for cell phones and smartphones. You can learn from them what your data the downloaded service is requesting access to. Be careful what you agree to.
- Provide only the necessary data to create an account.
- Instead of Facebook tracking, use newsletters and RSS feeds.

Don't Overshare



- No online shopping e-tailer needs your Social Security number or your birthday to do business.
- However, if crooks get them and your credit card number, they can do a lot of damage. The more scammers know, the easier it is to steal your identity.
- When possible, default to giving up as little personal data as possible. Major sites get breached all the time.

Time for Question...

Do you know of any tricks to prevent your information from being tracked?



Time for Answer...

Change settings to block trackers, use incognito mode, use VPN, use private browsers. Search Encrypt uses encryption to hide your search history from others who may use your device after you search.



Problems with online, card purchases and money transfers.

Safe use credit and debit cards

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

Participants will be sitting in the circle. Trainer on the flip chart will be writing giving guiding questions to the participants helping them to come up with rules to use credit and debit cards safely (appendix below).

Appendix

- Better use mobile payment application
- Use safety features provided by the card issuer.
- If you lose your card, inform the bank immediately
- Do not show your card in public.

Skip the Card, Use the Phone



Paying for items using your smartphone is pretty standard these days in brick-and-mortar stores, and is actually even more secure than using your credit card.

Using a mobile payment app like Apple Pay generates a one-time-use authentication code for the purchase that no one else could ever steal and use.

Plus, you're avoiding card skimmers—hell, you don't even need to take your credit card with you if you only go places that accept phone-based payments.

How does that matter if you're online shopping? Many a phone app will now accept payment using Apple Pay and Google Pay. You just need your fingerprint, face, or passcode to make it happen instantly.



Create Strong Passwords

- Making sure that you utilize uncrackable passwords. It's never more important than when banking and shopping online. Our old tips for creating a unique password can come in handy during a time of year when shopping around probably means creating new accounts on e-commerce sites.
- Even your perfect password isn't perfect. The smarter move: use a password manager to create uncrackable passwords for you. It will keep track of them and enter them, so you don't have to think about it.



Leakage of personal data, creating strong passwords, password organizers



Game: I have never ever...

Materials

Telephones/tablets/laptops with Internet access, projector, sheets of paper, pens, cardboards

Directions

- All participants stand in a circle. Statements beginning with "I have never..." are said and the participants who have made this statement must move one step forward. Then they return to their places. Here there are some examples, but the participants can also say any statement they want.

- Never have I ever shopped online
- Never have I ever been scammed on internet.
- Never have I ever talked to someone online without knowing him/her
- Never have I ever forgotten my passwords
- Never have I ever received a spam email
- Never have I ever been attacked by malware
- Never have I ever received an email asking me for all my personal information
- Never have I ever tried to find out someone's password
- Never have I ever suspected that someone had broken into one of my accounts.
- Never have I ever found an advertisement on my phone of something I had just searched for.
- Never have I ever suspected that I was being spied via Internet
- Never have I ever stalked anyone
- Never have I ever suffered cyberbullying



Leakage of personal data, creating strong passwords, password organizers



Game: I have never ever...

- Never have I ever cyberbullied anyone
- Never have I ever accessed suspicious websites
- Never have I ever downloaded a virus while trying to download something else
- Never have I ever had to change all my passwords
- Never have I ever had to change my credit card because its details had been leaked
- Never have I ever pretended to be someone else on the Internet
- Never have I ever ignored the rules for keeping a secure password.
- Never have I ever participated in a fake raffle on the internet
- Never have I ever lost all my work or anything important because I didn't have a backup copy
- Never have I ever clicked on a banner that said I had won a prize
- Never have I ever surfed the Deep web
- Never have I ever shared private information on social media
- Never have I ever shared embarrassing images on the internet
- Never have I ever posted offensive comments on the internet
- Never have I ever received offensive comments on the internet
- Never have I ever tried to find out someone's private information
- Never have I ever used two-step authentication
- Never have I ever used VPN
- Never have I ever felt unsafe on Internet



Leakage of personal data, creating strong passwords, password organizers

Game: I have never ever...

What's happening?

Game Never have I ever. About Internet topics.

All participants stand in a circle. Statements beginning with "Never have I ever..." are said and the participants who have made this statement must move one step forward. Then they return to their places. There are some examples, but they can also say any statement they can think of.

Privatize Your Wi-Fi

- If you're shopping via a public hotspot, stick to known networks, even if they're free, like those found at Starbucks or Barnes & Noble stores.
- Any of the providers in our roundup of the Fastest Free Nationwide Wi-Fi can generally be trusted, but you should probably also use a virtual private network (VPN) to be safe (here's why).





Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Presentation

Materials

telephones/tablets/laptops with Internet access, overhead projector, pens, markers, flipchart, ticky notes, A4 sheets of paper

Directions

Presentation of the information verification tool (CRAAP test), what it is used for and how to use it (appendix below) together with the Presentation.

Appendix

The CRAAP test is a test of the objective reliability of information sources in various scientific disciplines. CRAAP is an acronym that stands for currency, relevance, authority, accuracy, and purpose. The CRAAP test is designed to help teachers and participants determine whether their sources can be trusted. By using the test when evaluating sources, the researcher can reduce the likelihood of using unreliable information. The CRAAP test, developed by Sarah Blakeslee and her team of librarians at California State University, Chico (CSU Chico), is used primarily by higher education librarians. It is one of a variety of approaches to source criticism.

Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Presentation

It may be tempting to use any source in your article that seems to agree with your thesis, but remember that not all information is good information, especially in an online environment. Developed by librarians at California State University-Chico, the CRAAP test is a useful checklist to use when evaluating an online resource (or ANY resource). The test provides a list of questions to ask yourself when deciding whether a resource is reliable and trustworthy enough to be used in a research paper.

The CRAAP test is an acronym for: Currency, Relevance, Authority, Accuracy, and Purpose. It is not easy to determine if a source is trustworthy and can be used as a research tool. The test saves the time and energy needed to evaluate content available on the Internet.

Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Presentation

Resources must pass through five stages of verification.

Currency - timeliness of information

The time the information was published or posted, whether the information is updated or corrected, and whether the link works or not.

Relevance - the relevance of the information

Checks whether the information is related to the topic, whether the resource is relevant, and whether it can be used in academic work.

Authority

Builds trust by providing details about the author, publisher before trusting the information and the website.

Accuracy

Pay attention to the accuracy of the content. Information must be based on evidence presented to the audience. Language tone, grammatical and other typographical errors should be checked.

Purpose of the information

Determine the purposes of the information: inform, teach, sell, entertain or persuade.



Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Quiz

Materials

telephones/tablets/laptops with Internet access, overhead projector, pens, markers, flipchart, ticky notes, A4 sheets of paper

Directions

Divide the group into teams of about 4 people. Ask each team to find an article on one topic of their choice. Pick a topic that fits the group (appendix below). Distribute the printed craap tests (appendix below) and hand out to each person. Ask the participants to read the article, then have them analyse the whole text in the light of the questions included in the test. On the right hand side they have space for thoughts/conclusions/answers. Based on the test, they will determine how reliable the article is. There is no grading scale or number of points.

People work "online" on the received material, which means they can conduct an in-depth analysis of the material - learn about the entire article, look at its source in more detail, verify the data used, learn something about the author, etc. It is important for them to check, using the criteria given in the craap test, whether the material is credible, which elements indicate credibility and which undermine it. The participants can also write down their thoughts, which will facilitate the discussion. Ask each group to briefly present the results of their analysis.



Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Quiz

Appendix

Topics for groups:

Climate

Coronavirus

Refugees

Vaccines

Celebrities

Sports

European Union



Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Quiz

		Notes / answers
Currency timeliness information	When was the information published?	
	Has the information (if not new) been updated?	
	Does the case for which you are reviewing this information require more recent, up-to-date data, or can you rely on older material?	
	Do the links (if any), posted in the information work?	
Relevanc materiality of the information in relation to your needs	Does the information even relate to the topic you are addressing or answer a question that is important to you?	
	For whom was the information prepared? For which target group?	
	Is the information at an adequate level for your needs? Is it too basic and general or too advanced and detailed?	
	Did you check other sources of information before deciding to use just this one?	



Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Quiz

Authority origin of the information	Who is the author, publisher, source or sponsor of the information?	
	What are the credentials of the author of the information? What organization, entity, institution is he/she affiliated with?	
	Is the author qualified to write on this topic?	
	Can you find contact information, e.g. publisher name, email address, etc., next to the information?	
	Does the Web site address where the information appeared say anything about the author or sender (e.g., URL ends in .com, .edu, .gov)?	
Accuracy reliability, truthfulness and accuracy of information	Where does the information come from?	
	Is the information provided supported by evidence?	
	Has the information been peer-reviewed or cited (applies primarily to scientific papers)?	
	Are you able to confirm at least some of the information given in another source or using your knowledge?	
	Does the language or pronunciation of all information indicate impartiality and is devoid of emotional coloration?	
	Are there spelling, grammatical, or stylistic errors in the situation?	



Fake news - that is, searching the Internet, verifying information provided by the media.

CRAAP Test - Quiz

Purpose
purpose of
the information, the reason it was created

What was information created for?
To educate, inform, entertain, persuade?

Has the author or the person funding the creation of the information made it clear what the purpose of the information is?

Is the information a citation or description of facts, does it present an opinion, or does it have a propaganda character?

Does the viewpoint presented in the information give the impression of impartiality and objectivity?

Do you see elements in the information that indicate bias, taking a particular position, on issues related to politics, religion, worldview, or for example, presenting the perspective of only one institution or person?