STAYING SAFE ONLINE

YOUTH AND DIGITAL SECURITY

www.globalmoneyweek.org

GLOBAL MONEY WEEK

FINANCE DENMARK

Child & Youth Finance International

For teachers: How to use the booklet
This booklet on digital security includes many details. Choose which parts your students will be taught and try to have an open dialogue on these topics in class.

Global Money Week (GMW) is a global celebration, initiated by CYFI, with local and regional events and activities aimed at inspiring children and youth to learn about money, saving, creating livelihoods, gaining employment and becoming an entrepreneur. GMW takes place every year during the second week of March.

Read more: **www.globalmoneyweek.org**

Child & Youth Finance International (CYFI) is a global system change organization working with partners in over 130 countries. We have taken on the challenge of ensuring that everyone works together to reshape financial systems in order to economically and socially empower children and youth worldwide.

Read more: **www.childfinanceinternational.org**

This booklet "Staying Safe Online – Youth and Digital Security" is a moderated and international version of the original Danish booklet "Unge og Digital Sikkerhed" which is used in the Danish Money Week from 2017 and beyond.

Editor of original version: Troels Juel, consultant in Finance Denmark.

Original version is written in corporation by a series of Danish organizations and institutions: Finance Denmark, The Danish Police, The Agency for Digitisation, The e-mark, The Media Council for Children and Young People in Denmark.

Photos: Front page: Aleksandar Goergiev/Getty Images.
Page 3: Maskot/Getty Images.
Page 10: Bloom Productions/Getty Images.

March 2017

INTRODUCTION

Why digital security is important
Today, a large part of your life occurs online. When you share photos on Instagram or via SnapChat, transfer money to your friends through mobile apps or shop online for a new pair of sneakers or jeans; it all happens digitally.

With the world rapidly moving towards digitalization, new exciting opportunities are continually being created and become available to us all.

Nevertheless, it is important that you know more about these new opportunities and are aware of the challenges they may bring. These new challenges can be anything from how best to handle money online or to how to create a safe (unique) password.

This booklet was created to help you navigate the digital world of money in a safe way. Below 3 important basic rules when it comes to your on-line safety:

1. The first and most basic rule is to use common sense when you are online. If you see an unusual link or a website that does not seem safe, ignore it and close the window – best not to visit it!

2. If an offer on-line looks too good to be true, then it likely is too good to be true.

3. If you use the same password for all of your online accounts, you immediately become very vulnerable; if someone manages to gain access one account, they will also be able to access all your other accounts.

Just a few simple tips we will tell you more about in this booklet. Don't get us wrong, use apps and social media all you want. The internet is great for connecting with your friends, find information and share. Digitalization makes our lives easier and much more efficient. However, if you want to strengthen your online safety, it starts with you: use common sense when you go online.

This booklet will help you with your future online experiences and brings together valuable and practical advice for your digital safety!

Enjoy!

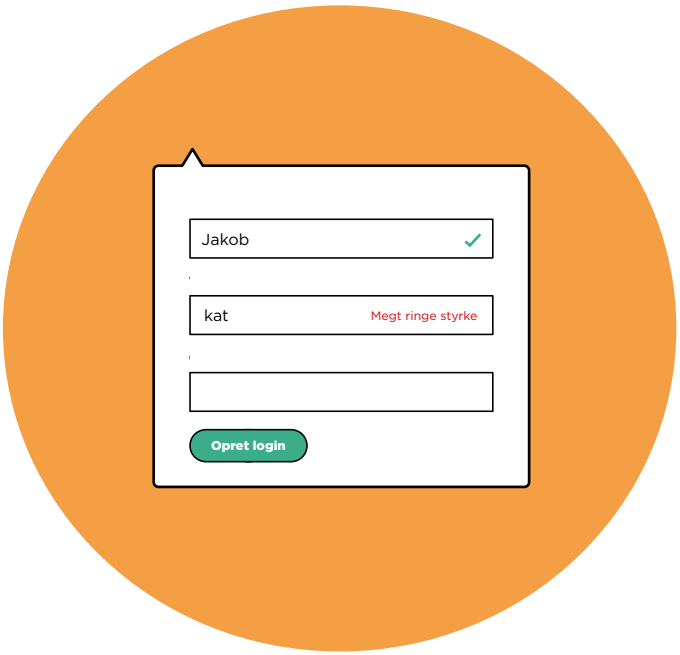
Child & Youth Finance International (CYFI)

CONTENTS

PASSWORD

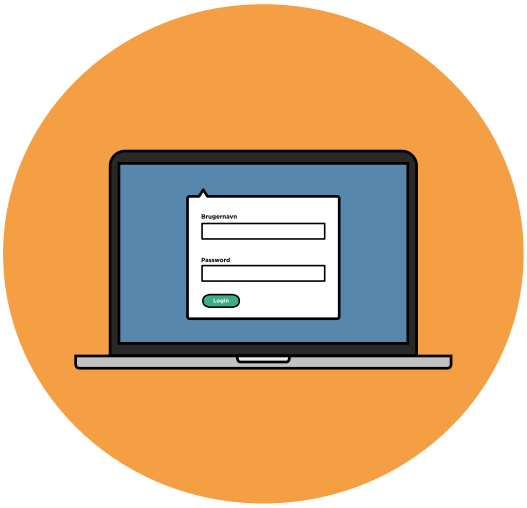
HOW TO MAKE A STRONG PASSWORD

Having a strong password is vital to your security online. It is important not to use any of your personal information when you create passwords - particularly if that information is readily available on any of your social media accounts. In other words, you should not use the title of your favorite movie, the name of your favorite football club, your mother's name, your cat's name, your date of birth, etc. Additionally, you should avoid using common and easy to guess passwords. Two of the most commonly used passwords are '123456' and 'password'. In general, it is best to create as much variation as possible in your passwords. That is, use both upper and lower case letters in combination with numbers and symbols.



Use different passwords

It is possible that you have several different online accounts, all of which require their own password. Some people believe that it is too difficult to remember all these different passwords – so they only use one and the same password for everything. In reality, memorizing passwords just requires a little practice. If you only use one password for all of your accounts, hackers and thieves can more easily gain access to all of your accounts and cause you serious problems.



Learn how to construct good passwords

The length of a password is important if you want to create a strong password. Your password should always be at least 8 characters, even if the minimum requires less. In addition to the length, secure passwords also include a mixture of uppercase and lowercase letters, numbers, and symbols. This combination of characters makes it harder for others to successfully guess your password.

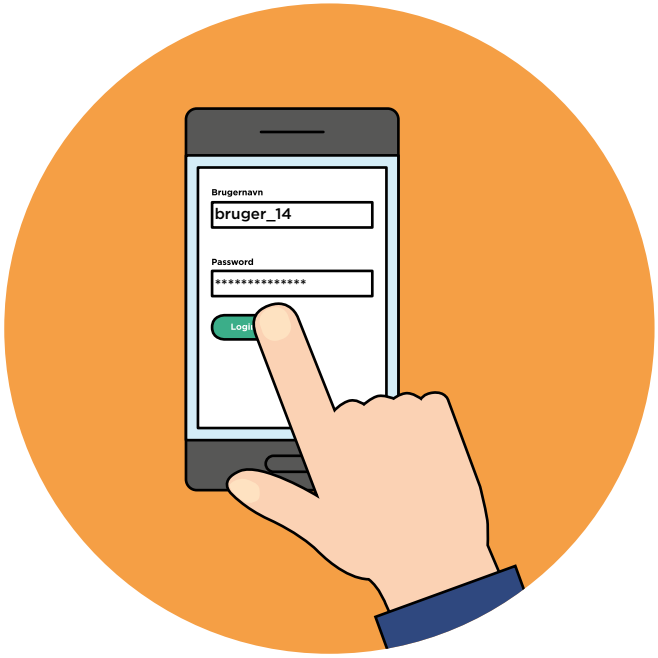
Think of phrases
One trick which you can use for creating a safe and secure password is to try to think of a passphrase instead of a single word. A passphrase is a short proverb or part of a song that you can use to build a strong password.

For example, you can use a verse from a song and use the first letter from each word to create your passphrase. Then, you put it into an order that is easy to remember (singing as you type). You can also use special characters, uppercase letters and numbers in different parts of the password - and not only at the beginning or the end. For example, "NgGyU!nGlYd!1" (Never gonna give you up, never gonna let you down) would be a strong password that is also easy to remember.

A password should be easy for you to remember and hard for others to guess.

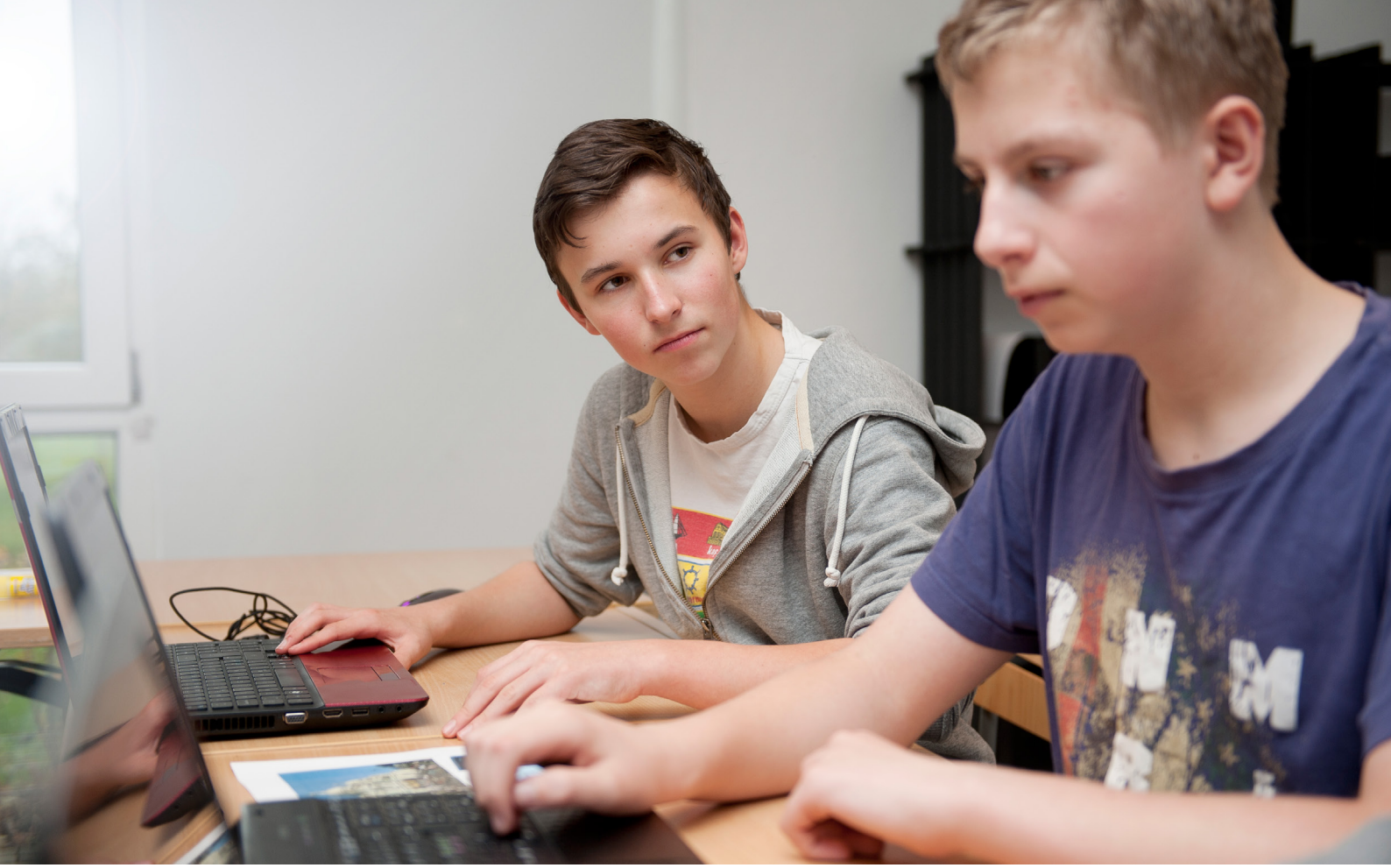
Make your lock pattern passwords safe
Creating a safe lock pattern password on a device (patterns are mainly used for logging in and confirming app purchases) is as important as a good password with different numbers, letters, and symbols. Unfortunately, many people do not make good lock pattern passwords. 44 percent of pattern passwords were found to start in the upper left corner. 10 percent of locking patterns were also found to be shaped like a letter, usually the first letter of a family member's name.

A safe pattern code consists of a pattern of lines that cross each other. It is important to disable the "make pattern visible" option so that no one around you can see the pattern as you enter it.



Factbox: here are the most commonly used passwords in the world in 2016:

1. 123456
2. password
3. welcome
4. ninja
5. abc123
6. 123456789
7. 12345678
8. sunshine
9. princess
10. qwerty



WHY ARE PEOPLE CHEATED BY CYBER CRIMINALS?

Cyber criminals have become increasingly organized, clever, and strategic in their attempts to gain access to the accounts of others. Their methods are creative and can sometimes be very difficult to immediately figure out and recognize as a scam. Furthermore, cyber criminals are constantly finding new ways to fool people.

Many young people do not change their passwords

It is important to remember that online scams have unfortunately become a part of our everyday lives. Cyber criminals take advantage of the fact that people frequently recycle their passwords. This means that the criminals only need to hack a single password to gain access to several accounts.

FACTBOX:

Do not use your birthday or the names of family members or pets in your passwords. It is too easy for others to guess!

DISCUSS IN CLASS:

How do you ensure that others have a difficult time guessing your passwords?

Do you suspect that someone has guessed your password?

If so, change it immediately!

SOFTWARE

SOFTWARE ON YOUR MOBILE, TABLET AND COMPUTER

What is a device?
Device is a commonly used term for your computer, smartphone and/or tablet. So a device is a common name for all gadgets and apparatus which you can use to go online or which you can install apps on.

What is malware and hacking?
Malware can be translated from the term malicious software since it is a contraction of the words malicious and software. It is a common term for programs that cause harm to your devices.

Hacker(s) is the term used for people who purposefully exploit security holes in computer, mobile, and tablet devices or through personal, professional, and business web accounts to gain access to other people's personal information, data and images. Hackers may use malicious programs with spyware and malware to infiltrate some of the most advanced computer security systems.

You use your mobile, tablet and computer devices all the time. Furthermore, the possibilities of how you can use these devices is constantly evolving. For example, you can now not only communicate online with friends and family, but also now with the school doctor or your bank conveniently from your devices. Also, you can now shop online directly via apps on your tablet and you can pay with your phone in supermarkets. There are ways for you to make it much harder for criminal hackers to get hold of your personal information or money. This section focuses on software that protects your devices from malware, viruses, and hacking.

TIPS AND TRICKS FOR HOW YOU CAN KEEP YOUR DEVICES SAFE FROM HACKERS AND VIRUSES:

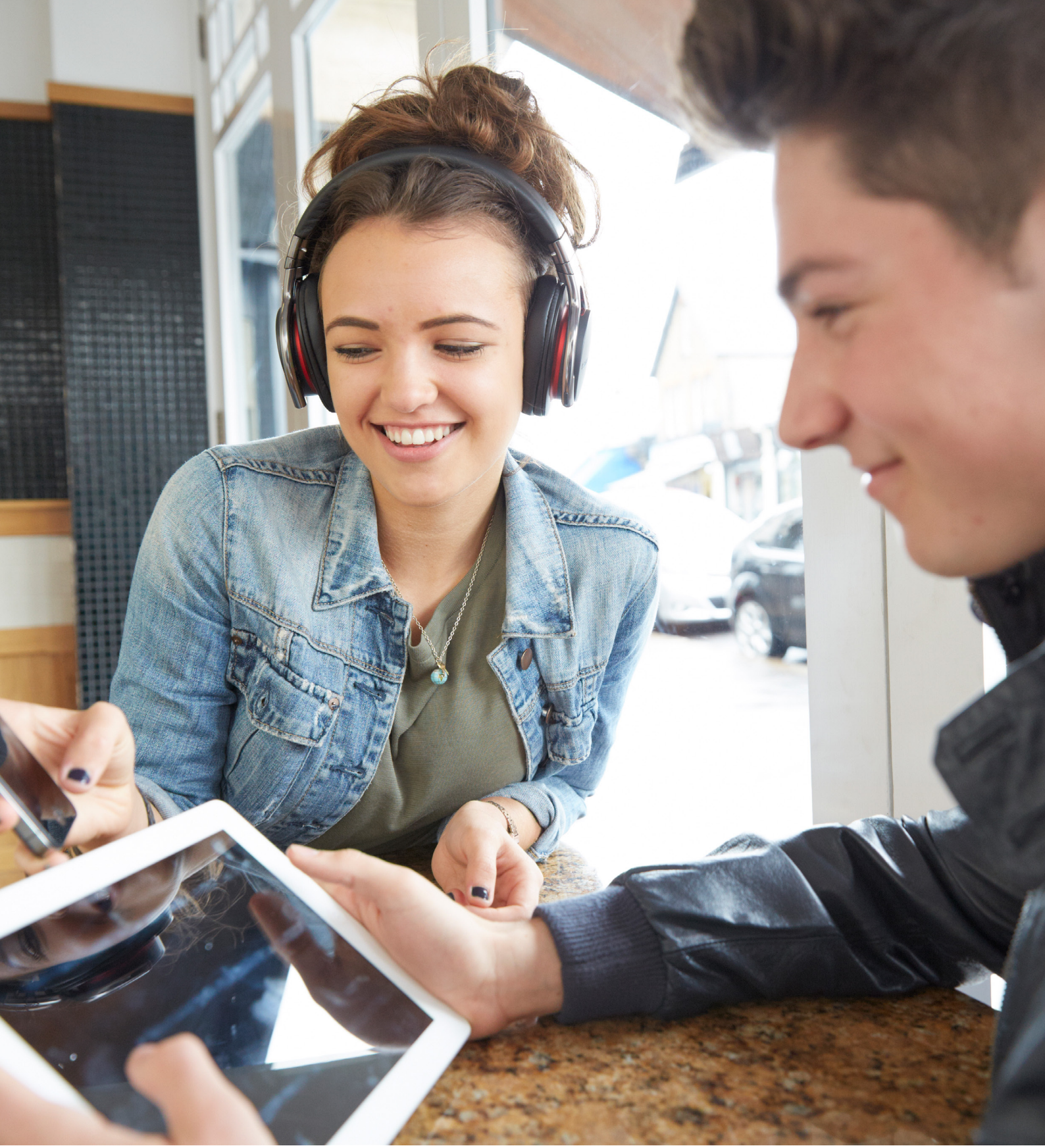
Please update
Most devices do not typically automatically update apps or security software. Fortunately, it usually does not require much time to update your apps and security software to ensure you have the most up-to-date protection on your devices. It is usually advisable to update your device immediately when it is to address any bugs or viruses. However, for some updates, it is best to wait a day or two until reports of any possible security vulnerabilities become available.

If your devices are not updated with the latest software, they may be more vulnerable to hacking, malware and virus attacks. This means that foreign entities can steal information from your device (e.g. passwords and credit card data) or even completely take over your device.

Use antivirus software
Antivirus programs help keep harmful files out of your devices. There are several free programs you can download and install. However, if you would like to further bolster the protection of your devices, you can also pay for more effective antivirus programs. Paying for a certain antivirus program may be money well spent since they typically include features that are not available with free antivirus programs. Talk to your parents about the possibility of buying a package with multiple licenses so you can protect several devices at once.

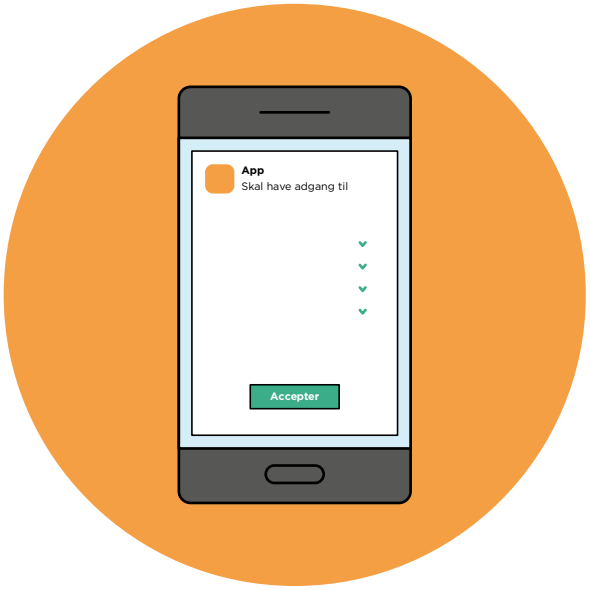
Be cautious of open wifi networks
It is likely that you have your devices set up to automatically log in to the wifi networks in your home and the places you most frequently spend time at. It is certainly easy, fast, and convenient to have it set up this way. It is also a smart and easy way to save on data usage. Thus, it is also tempting to log in to free and open wifi networks when you are out in the city or elsewhere. However, it is important to only use wifi networks where you know the host can be trusted. If you use an open wifi network where you do not know the host, you may run the risk of unauthorized people monitoring your online activity and intercepting your personal information.

Many shops, cafés and restaurants offer open networks to their clients. If an attacker is on this open network, they may be able to easily observe and/or steal the information that is sent to and from your device. Therefore, it is pertinent to be cautious and aware of what wifi networks you log on.



Do you know what you are downloading?
You may often download new apps for your mobile, tablet and computer. When you use the authorized services such as Appstore and Google Play to download new apps you can be fairly certain that your downloads are not filled with viruses or malware (Important: Be aware that not all apps and programs via authorized services are thoroughly tested for viruses and malware).

However, it is not advisable to download apps and software directly from links in emails and messages as they may contain viruses and malware. Additionally, if something is free, but you know it usually costs money, it is possible that it contains viruses or malware.



Giving apps permission?
When you download apps, you may also be granting these apps permission to access a variety of information on your device. Certain apps may ask for permission to things that are not necessary for the operation of that app. This can sometimes include access to your camera and microphone at any time. It's a good idea to view the settings of the apps on your devices to inspect what permissions you have granted them.

DISCUSS IN CLASS

Why is it important to update devices?

How often should they be updated?

Think over which wireless networks you should and shouldn't use?

Have you heard of someone who was hacked? What happened?

How will you change your behavior when using devices?

What advice would you give to others?

How will you ensure that you use your devices more safely?

DIGITAL MONEY

TAKING CARE OF YOUR MONEY ONLINE!

Money is now not only used in the form of physical currency, it is increasing being used digitally! Many people now use mobile banking, online banking, and MobilePay. With web or mobile banking, one can easily and conveniently transfer money to other people, pay bills, and/or transfer money between accounts. There are differences between mobile banks, but they all typically require a specific ID number to make payments to other accounts.

It is essential that you make sure that others can't use your web or mobile banking app. You can contribute to doing this by ensuring that no one is aware of your passwords, secret questions and answers, or any other codes.

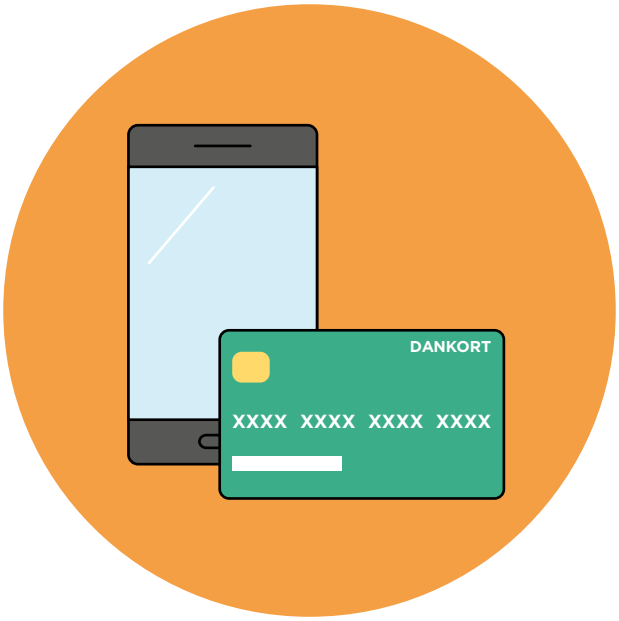
MOBILE PAYMENTS

You should be confident that when you send money digitally that it is sent to the correct recipient. Additionally, you will want to confirm that the amount you send is correct. It's no fun to unintentionally send 250€ if you just needed to transfer 25€. Always remember to double check that the information of your online payments is correct.

Mobile payment solutions are personal and should only be used by you. Thus, unless you have complete trust in someone (e.g. your parents), it is important that you do not let others have access to your phone without you being able to see what they're doing.

Take care of your PIN

You must wisely choose a PIN for your mobile payment apps. It is important that you make sure that others do not discover your codes (e.g. you should not write it down or keep it stored in the notes on your mobile phone). It is also not wise to take a picture of your PIN and have it stored on the camera roll in your mobile. It would be a treat for any hacker to come across your PIN if they gained access your device. If someone hacks into your phone, they will immediately gain access to all the codes that you have pictures of, if you have any saved.



PAYMENT CARDS

A debit card can be used for purchases in places such as stores and online shops or they can be used to withdraw cash from ATMs.

A payment card is personal and has an a 4-digit code that you enter when you use it. It is important to ensure that others do not discover your code. For example, make sure that others cannot read over your shoulder when you type your code. It is wise to keep one hand up in front of the keyboard when you type your code, especially if there is a queue behind you.

Similar to online payments, it is also advisable to confirm that the amount you are paying matches the actual amount of your purchase. While the vast majority of clerks and cashiers are trustworthy, an untrustworthy person could add extra onto your payment. Therefore, it is wise to always double check the amount you are paying is correct and to get a receipt for your purchase.

If you lose your debit card – or believe that your account has been compromised – you should immediately contact your bank.

i

What types of payment are you familiar with?

There are different types of payment cards, such as debit and credit cards.

With debit cards, your purchases are immediately deducted from your account, or no later than the next business day. Therefore, it is typically banks that issue debit cards since it is necessary for the cards to have direct access to the user's bank account.

Several banks offer debit cards with limits (balance control). This feature does not allow you to spend more than a specific daily or weekly limit, or spend money that is not in the account. Examples of some cards with balance control are MasterCard Debit, Maestro, and Visa Debit.

A credit card is a similar to a debit card in that you can make purchases in stores and online without using physical currency. However, they do not use money directly from your bank account(s). Instead, the money used for purchases is from the company that issues that credit card and you are required to pay the creditor back within a certain timeframe. Credit cards typically require minimum monthly payments to be payed or else the amount owed accumulates interest or a late fee will be added. Examples of credit cards are MasterCard, Diners Club and American Express.

i

Have you lost your debit card or do you suspect that it has been compromised?

If so, call your bank immediately.

ONLINE SHOPPING

People around the world are increasingly doing their shopping online rather than in person. This is because the web offers the convenience of shopping from home and it makes it easy to find the latest products and bargains. Unfortunately, the world of online shopping is also a place where swindlers try to cheat customers – particularly those who do not use their common sense when buying products. Therefore, we have written seven pieces of advice that you can use when shopping online to help you avoid having any negative experiences with online shopping.

CHECK WHERE THE WEB SHOP IS BASED

Do you visit online shops that are based outside of the EU or your country of residence (if you live outside of the EU)? If so, you risk having to pay customs. Having to pay customs will make your purchase become more expensive than what you anticipated. Consequently, what was originally a bargain price for a product may not be such a bargain in the end. Keep this in mind when shopping online.

Look for the padlock in the address bar
Is there a little green padlock next to the web shop URL? The green padlock means that the information you enter about yourself and your payment method is transferred through a secure connection. Do not make purchases on online shops that do not feature the green padlock next to the URL.

Read about others' experiences with that online shop and product
Once you have found the right product at the right price, it is worth your time to investigate what previous customers say about this product or online shop. Thus, it is a good idea to look at user reviews found on the online shop and elsewhere on the web. Just remember that online ratings can be manipulated, so it is wise to use your common sense when inspecting user reviews. Moreover, you should never let user ratings alone form the basis of your purchase. Instead, view them as a good addition to helping guide your online purchases. If something doesn't feel right about the online shop or product, ask a trusted adult for their opinion or look elsewhere online to buy what you want.

Always read what you are saying yes to
It may not be very exciting, but you should always read the terms and conditions of your online purchases. Terms and conditions can differ from site to site. Especially when it comes to details on payment, complaints, and/or any specific conditions related to shipping. The terms and conditions should also notify you on subscription policies and rules regarding returns and exchanges.

Check and know your rights
In the EU, you have 14 days to return any items purchased on the web. This means that you can exchange or receive a refund for the shoes you just bought if they are too large, or for other

reasons if you do it within the appropriate amount of time. Typically, you must pay for return shipping if you regret your purchase or made a mistake. Read the terms and conditions before your purchase so that you are aware of the return/exchange shipping costs.

Always pay by card or MobilePay
No matter what online shop you shop with, it is safer to pay with a credit card or with MobilePay Online.

Save the receipt
If the product you bought suddenly fails after five months, you stand the best chance of receiving a replacement or partial refund if you saved the receipt and/or order confirmation from the webshop. Saving the receipt or order confirmation number makes it easier for companies to find your purchase in their system. It is wise to always save receipts for at least two years.

DISCUSS IN CLASS:

Have you shopped online before?

What was your experience like?

DISCUSS IN CLASS:

Have you heard of someone who was deceived online before?

What happened?

Learn to spot a fake shop!
Most online purchases occur without any problems. However, as with everything else in life, sometimes problems do occur. There are a few online stores that do not follow the rules and try to scam the buyer. Fortunately, particularly if you know what to look for, most scammers are rather easy to spot. While there are several different things which could suggest that an online shop is illegitimate, there are four easy to observe warning signs that indicate that you should stay away from an online shop:

Prices that are too good to be true: Many scammers advertise huge savings on popular brands like Nike, RayBan and Gucci. A scammer may only charge 40€ for a pair of sneakers that normally costs 200€ in order to make some quick and easy money. Always remember that if the price of a product sounds too good to be true that it most likely is.

Peculiar prices: Online shops that try to scam you often use a price converter from specific currencies. Therefore, if you encounter quirky prices such as 468.34€ rather than 499.99€, it is possible that that shop is not reputable. Most reputable sites feature more common combinations of numbers such as 500€ Or 499.99€. This is not always the case but it is something you should be aware of when shopping online.

Language errors or spelling mistakes: Many non-reputable online shops translate all of their text from another language via computer translation programs. Therefore, if you see the description of a product is full of grammatical errors and/or spelling mistakes, it is likely best to avoid that website.

Suspicious URLs: Always check to see if the URL matches the name of the online shop. Many shops that try to scam you take over old URLs that do not have anything with the goods being sold.

SOCIAL MEDIA

GOOD BEHAVIOR ON SOCIAL MEDIA

DISCUSS IN CLASS:

Discuss in class what social media everyone uses, why they use it and what they think is smart practice on social media. Also, talk about what they've heard about others' good and bad experiences on social media.

Most people use social media and have accounts on two or more platforms. Even if you do not have any social media accounts, you are well aware of the social media platforms you could join. When you are online, it is always important to consider what you write since it is possible that what you are writing will be seen by others or shared later without your knowledge. A good rule to maintain is to not write anything online which you would not say out loud in public. Even if you are joking, it can be difficult for others to tell that you are joking and they may interpret your humor as inappropriate. Moreover, besides what you are saying, you also need to be aware of what information you share online, do not reveal personal information and do not share or re-share images or videos without permission from those involved.

IS SOCIAL MEDIA FREE?

It is free to create a profile on the majority of social media platforms. However, these mediums are owned by private companies that continually desire to make more money. One way in which they make money is by collecting information about you – such as your browsing habits - so advertisers can more easily target you. The information which you provide when you create a profile on their site and all of the information that you provide when you go on social media expand your digital footprint. Your digital footprint (i.e. all the posts you like, click, comment or share) is constantly being tracked, stored and used. Social media platforms use your data to generate a profile of you so they can target you with specific content and ads.

TAKE CONTROL OF YOUR DIGITAL LIFE

When you create an account on a social media platform, your profile is typically set to the default setting of being able to be viewed by anyone and everyone. It is important that you are aware of this and are careful about what you share on social media and elsewhere on the web. To make what you share online more difficult for strangers to view, modify the privacy settings on your profiles so that only your "friends" or "followers" can view your profile and the content you share. You should also consider whether or not it is necessary for you to share information such as your school, birth date or phone number on your profiles. If it isn't necessary, it is wise not disclose it.

It may not be wise to share that information anyways. Also, it is important to always think twice about what you share online. Even if you delete what you wrote or shared quickly after posting it, you can never be sure that that information is completely gone or that someone else did not record it while it was online.

HINTS

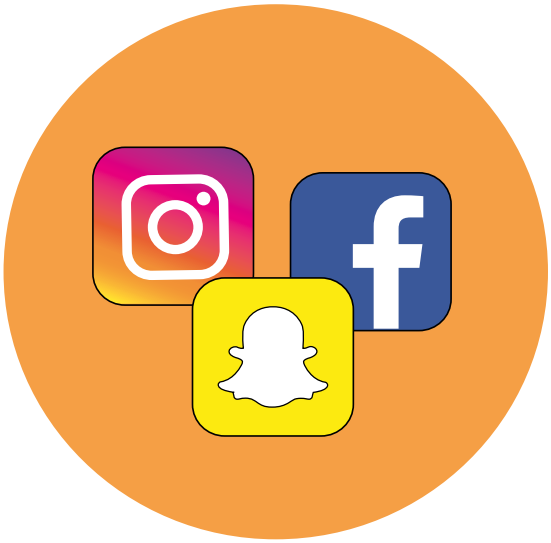
Always be sure to modify the privacy settings on social media so that only your “friends” or “followers” can see what you post. Remember that you can also block specific people or groups of people from viewing your profile.

Speak clearly online and use appropriate language as misunderstandings can easily occur when you are not communicating face to face. Think twice about what you like, comment on and share as rumors and lies can spread quickly and your reputation could be easily damaged.

Do not share photos or movies of yourself with significant others that you do not want others to see. It is easy for others to save these pictures or videos or even reshare them without your knowledge. Even if you have a strong and positive relationship with this person now, it is possible that you may not in the future.

Never share or reshare private pictures or movies of others without their explicit permission, even if you think the picture or video is sweet or funny. The person in the picture or video may think that it is embarrassing or they just do not want to be featured online. Always ask for permission before shooting and sharing. Also, respect others when they say no.

It is easy to get carried away and share a fun, exciting or sexy picture or comment. However, as always, think twice before posting or sharing anything. If you regret a comment or a picture, delete it immediately. If you shared it with others, ask them also to delete it. You can always ask a friend, family or teacher for help. Remember to apologize if you've done anything inappropriate or hurtful to others.



www.globalmoneyweek.org

www.childfinanceinternational.org

GLOBAL MONEY WEEK

FINANCE DENMARK

Child & Youth Finance International