Erasmus+

PROJECT: YOLLO BUT MOLLO – INTERNET SAFETY EDUCATION IN SCHOOL
PROPOSAL FOR GOOD PRACTICES ANALYSIS

A BRIEF OVERVIEW ON INTERNET SAFETY IN SCHOOLS

SCHOOLS PLAY A KEY ROLE IN PROMOTING INTERNET SAFETY. A WHOLE SCHOOL APPROACH TO E-SAFETY CAN HELP INVOLVE STAFF, GOVERNORS, PARENTS AND PUPILS THEMSELVES IN KEEPING CHILDREN AND YOUNG PEOPLE SAFE ONLINE. DIGITAL TECHNOLOGY IS CONTINUALLY CHANGING SO IT IS IMPORTANT THAT SCHOOLS STAY UP-TO-DATE WITH NEW DEVELOPMENTS. AS INTERNET USE HAS BECOME A DAILY PART OF MOST STUDENTS' LIVES, STUDENTS MUST KNOW HOW TO PROTECT THEMSELVES AND THEIR IDENTITY AT ALL TIMES—ESPECIALLY WHEN TEACHERS AND PARENTS AREN'T THERE TO HELP THEM.

TEACHING STUDENTS ABOUT INTERNET SAFETY HAS BEEN IMPORTANT FOR AS LONG AS THE INTERNET HAS EXISTED. TEACHERS MUST TAKE CARE TO EDUCATE STUDENTS ABOUT PROPER ONLINE BEHAVIOUR, CYBER BULLYING, AND SOCIAL NETWORKING SITES.

MOST SCHOOLS ASK PARENTS TO SIGN A PERMISSION SLIP WHEN THEY ADD INTERNET ACCESS TO THE RESEARCH TOOLS AVAILABLE TO STUDENTS. MOST SCHOOLS ALSO ASK STUDENTS TO SIGN A CONTRACT PROMISING TO FOLLOW AN OUTLINED SET OF RULES COVERING THEIR USE OF THE INTERNET AND THEIR ONLINE CONDUCT. THESE TWO PERMISSION SLIPS — WITH A STATEMENT OF WHAT THE INTERNET IS AND HOW IT WILL BE USED IN THE SCHOOL SETTING — ARE KNOWN AS AN "ACCEPTABLE USE POLICY (AUP)."

The decision to commit finances for computers and Internet access in individual schools often originates at the district level. As a result, many school districts have taken the initiative in drafting and adopting an Acceptable Use Policy.

Perhaps the greatest concern parents and educators have about Internet access is the possibility that students will encounter material that does not have educational value or that is "objectionable" for other reasons. Establishing your school's Internet policy and rules of conduct up front will help schools, parents, and students remember that Internet access is a resource privilege, not a right.

Our comparative study and resources can contribute to develop:

□ a trained workforce who are confident in online safety, identifying and responding to concerns

□ resources to teach children and young people the skills to stay safe online

□ resources and advice to share with parents and careers

□ robust e-safety policies and procedures, IT infrastructure and support and regular reviewing of your e-safety provision.

1.Schools’ Contribution Form

1. Description of the ICT current policy situation in each of the partners’ schools
2. The first serious computer procurement in the Macedonian schools was the donation of 5300 PCs that were installed in primary and secondary schools in the period 2003-2005. In all other schools of the partnership computers were already present in schools in larger numbers.
3. E-Schools Project (2003-2023)- Creation of 460 computer labs with PRC computers in all primary and secondary schools. Also, a series of training programs were conducted for most of the secondary and primary school teachers, focusing on use of ICT through project-based learning strategies and networking. Besides, a large number of teachers passed the training for using this software.
4. All schools from the partnership were equipped with computer laboratory with 5-20 personal computers, and each secondary school was equipped with one or two computer laboratories with 20-40 computers. Most of the time these laboratories were used for teaching and learning the regular subjects: Informatics in primary schools, and Informatics , Information technology , and Programming languages in secondary schools. Statistically in Macedonia there was one computer per 56 children, in the others from 32 to 45. The subject Informatics is obligatory in both primary schools or secondary schools.
5. More than 20 million euros were projected in the 2007 Budget in Macedonia. This project, called One Laptop per Child , is the largest and most important education project undertaken in the 16-year history of the Republic of Macedonia. The Macedonian government has opted to use Client - Server based technology rather than offer one laptop per child.
6. Within the ~~seco~~nd project, called "Macedonia - Country of Computer Experts", from May 2007 all the citizens have the opportunity to be trained for basic computer skills free of charge in partnership with private sector. Macedonians interested in upgrading their computer skills can get free training under a new government programme.

7. There are many things that moved the things in the right direction in the last years in the education in all countries of the partnership. The new computers and computer equipment, and broadband fast speed Internet are now reality in the most of the schools. This is a result of the outstanding efforts of the Governments, as well as, previous and current projects in the field of ICT in every school. The large-scale computerization of the education is a crucial part of the process of creating and development of the European Information Society.

8. The situation with software is quite different. There is an evident lack of educational software on Macedonian and Romanian language. The ToolKid package is a good example of such software, but its target groups are just K-4 teachers and students. The educational portal is also very useful, but it needs further development and improvements. This situation is a great challenge for university teachers, primary and secondary teachers, and business IT sector.

9. Teachers, parents, students, educational authorities, managers of the ICT projects in education, are the main actors in the process of computerization of the education. They are faced with many challenges: creation of education software and digital educational material, proper implementation of ICT in education for learning, teaching, managing and administering, trainings for teachers in the framework of their professional development and continuous education. We need the synergy of all actors, mentioned above, in order to follow the way of the developed countries.

2. Describe 5 good practices from your schools on the chosen topics

Macedonia
1 practice on methodologies for primary school
1 practice on methodologies for high school
1 practice on pedopornography prevention
1 practice on ICT addiction prevention
1 practice free

France
1 practice on methodologies for primary school
1 practice on methodologies for high school
1 practice on development of basic skills for primary school
1 practice on cyberbullying prevention
1 practice free

Romania and Czech Republic
1 practice on methodologies for primary school
1 practice on methodologies for high school
1 practice on development of basic skills for high school
1 practice on sexiting prevention
1 practice on e-security

Italy and Turkey
1 practice on methodologies for primary school
1 practice on methodologies for high school
1 practice on Internet and right
1 practice on grooming prevention
1 practice free

15 Strategies Educators Can Use to Stop Cyberbullying

The advent of technology has brought with it familiar problems in new forms. Yet cyberbullying is unique in many ways.

What makes cyberbullying so different than in-person bullying?

- It is often anonymous and unlimited by time and place so the victim has little respite from the abuse.
- There is an element of disinhibition due to anonymity where students who would not normally participate do so. It can reach hundreds or even thousands of people quickly. The victim can feel even more isolated.
- It often involves repeated episodes of aggression and an imbalance of power. The victim may feel escape is impossible.
- More females are the victims and perpetuators of this type of bullying.

As educators, we need to be specifically aware of cyberbullying. Why is it so important to address cyberbullying in schools first? The Center for Safe and Responsible Internet Use, argues that two thirds of school violence begins through social media. Cyberbullying can lead to school failure, psychological implications, depression, violence and illegal activity.

An Educator's guide to Cyberbullying and Cyberthreats defines the behavior as verbal aggression such as:

- Harassment or repeated insults through various forms.
- Defamation of a person's character through derogatory postings, rumors, or images.
- Flaming or fighting messages using anger and vulgar language.
- Outing or deceiving someone into sharing secrets or private information.
- Polling such as posting an image on a voting website to make fun of a person's looks.
- Impersonation or identity theft to embarrass or destroy a person's identity.
- Cyber Stalking including sending intimidating or threatening messages.
- Pedopornography including sexual solicitation and/or exploitation.
- Unsafe digital communities with shared interests, such as social communities that validate eating disorders, violence, or drug use.

Although the research about cyberbullying is still emerging, there is some consensus on best practices. There are a few things we can do as educators to curtail cyberbullying

1. Create digital citizens. Cyberbullying is impersonal in nature. It is important to teach kids that the same rules apply in and out of the digital world. Clearly teach students how to be cyber safe and savvy. CSRIU (the Center for Safe and Responsible Internet use) provides some free handouts tailored by grade level to teach students how to be safe online. Microsoft even provides a free instructional program to teach digital citizenship and ethical use of technology. Much like rules are taught, digital citizenship can be imparted through explicit teaching.

2. Raise awareness. Awareness is powerful. It changes social perceptions. Rather than create panic over technology use or spread misunderstandings, awareness allows a positive atmosphere to emerge. Put cyberbullying in the spotlight in your classroom.Teach students about the psychological and legal ramifications. Explore issues like technology risks, cyber safety and positive online communities. Talk about age-appropriate cases of cyberbullying and their resolution. Showcase how technology is being used to help people in your community. Show students how they can use technology for the greater good. For instance, a new trend is creating a managed space for classmates to compliment each other on school achievements or work together on a class project.

In 81% of violent incidents someone other than the attacker knew what was going to happen but did not report it.

1. Teach students it’s okay to report abuse. Students need to know that they should report abuse. The Columbine Commission report reported that in 81% of violent incidents someone other than the attacker knew what was going to happen but did not report it. It is important to break the silence surrounding cyber abuse. Victims often do not report abuse for several reasons:

 They fear retribution from peers.

 They have anxiety that adults will remove computer or cell phone access.

 They don’t think adults will know how to resolve the situation. Often, adults may respond by removing technology from the victim, which is often seen as a punishment. Let kids know it’s not technology that is the problem, but irresponsible use. Give examples of how situations where resolved that involved cyberbullying, so they trust turning to you.

2. Establish firm policies. Rules regarding technology need to be explicitly taught, rather than assumed. A student should be aware of policies before a problem occurs. Create clear boundaries. Policies serve as a good way to curtail verbal aggression and establish it as an unacceptable behavior. Policies should also be specific, including any legal implications. Here is an example of a written policy address pedopornography, that provides clear information.

3. Realize that younger generations identify more closely to their online presence. As an adult, it is easier to separate yourself from online interactions. But younger generations may have a more difficult time with this. What happens online is very serious to them, and they do not take it lightly. Their online persona is essentially the same to them as their real person. If a student approaches you about a problem, don’t try to minimize it. Find resources immediately and make it apparent that you understand it is a serious issue.
A webinar mentioned in the Examiner, “When Cyber bullying spills into schools” recommends using a 5 prong method (The 5 R’s) when addressing cyberbullying situations.   Respond always, Researchfacts, Record documentation, Report findings, and Revisitthe issue to make sure it is resolved.

4. Team Building.Team building is a powerful way to make groups behave cohesively. I once saw a group from the US Army go to a local middle school to do team building exercises. Using a rope and a few random objects, the students had to work together to lift an object. The purpose of the activity was to make all members of the class work together towards a common goal.They had to use all of their individual strengths and realize each person’s abilities were necessary to complete the task. Teachers might consider having a weekly class meeting or similar activity. Create activities that might involve students to socialize with others that they might not normally

5. Encourage education for teachers, administrators, and counselors. Cyberbullying problems frequently change due to the changing nature of technology. It's important to stay up to date. A recent study in Childrens & Schoolsfound that half of school social workers felt ill-equipped to handle cases of cyberbullying. Education is essential.Many free webinars and workshops are available to educate teachers. For instance, "Guarding Kids Against High Tech Trouble" provides great multimedia training resources. There are many paid consultants and non-profit organizations that provide free resources specializing in this area. Billy Belsey, the Canadian Educator who coined the term "cyberbullying" is one such activist who provides teacher training.

6. Get Parents Involved. Parents may often be unaware of cyberbullying, so it is important to report what is happening so that they can intervene at home. Some data suggests that blocking the person may be the best way to stop the abuse. A study by the Center for the Prevention of Violence, said that 70% of teens said that blocking cyber friends stopped the abuse. Educators might suggest parents buy filtering software or special phones for younger children and teenagers.

7. Establish open communication with students. Students need to know who and where they can go to before a problem occurs. By the time a situation escalates, it may be too late. Students may be so stressed with their situation that they may not be thinking logically. It's best to make resources clear and available before situations become muddled with stress. You can have an anonymous box to report cases so that students know they can feel safe to report information. Organizations such as Safe2Tell, allow students to report incidents anonymously. You might have your school establish a hotline, or contact a local organization.Knowing there is a way to report cases may also stop students from engaging in the behavior. Research suggests that a parenting style that is emotionally warm with clear limits best creates resiliency in regards to digital aggression. Teachers can follow the same example: Be clear, empathetic, and communicate openly with students.

8. Allow technology in school. By incorporating technology in the classroom, teachers can focus on the ethical use of technology. Prohibiting technology often makes the problem worse. The behavior goes further underground. Teaching students how to use technology appropriately is better than having them figure it out with no guidance.

9. Know when to use community resources. There may be situations that require the intervention of greater community resources such as counselors, administrators, and law enforcement. Cyberbullying needs to be taken seriously and getting the community involved may prevent larger problems.Offer counseling services to both victims and perpetuators. Let students know that it is okay to need to talk to someone. Some situations have legal ramifications, such as the distribution of child pornography and need to be reported to legal agencies immediately. Cyberbullying policies should focus on changing school climate.

1. Create a positive school environment. The National Bullying Prevention Campaign in the US, recommends establishing a school-wide approach that changes the overall climate of schools. It focuses on norms of behavior. One exceptional program at preventing violence is the Olweus Bullying Prevention Programthat focuses on improving peer relationships through a school-wide approach.It includes the support of classrooms through rules and class meetings. Some research suggests that cyberbullying may be more common in poor school environments. It is uncertain if these environments cause bullying or simply make it more acceptable. A positive classroom where individuals are appreciated and respected can spill over to the unity of the group and create a positive, understanding environment. Cyberbullying policies should focus on changing school climate.

2. Interventions should focus on restoration, rather than punishment. At times, punitive interventions increased retaliation to reporting students. Policies should hold aggressors accountable for conduct and focus on making amends. Addressing the situation in a healthy way avoids further incidences. These might include teaching students about healthy relationships, responsibility and empathy. It is vital to create opportunities for forgiveness and reintegration to occur. Punishment is different than restoration in that it focuses on the rule broken, rather than the overall behavior. Restoration aims to

o Acknowledge the behavior.
o Understand the harm that was caused to the person.
o Repair or amend the harm in some way.
o Commit to change so it does not happen again.

3. Establish a baseline. Some studies and programs suggest having students participate in anonymous School Climate Surveys to see the extent of bullying and other types of behaviors occurring in the school. Red flags can be identified. This can give administrators clues as to what types of things to look for and address. You may want to do this in your own classroom.

4. Zero tolerance policy. Make students understand early on that bullying of any kind, including cyberbullying is unacceptable. The Massachusetts Aggression Reduction Center, found that students reported “looks, not fitting in, and sexual orientation” as reasons for being targets. Students with disabilitieswere more likely to be targets of cyberbullying, than in person bullying.Teach students about being responsible world citizens who are accepting of individual differences. Make sure that groupings in the classroom allow students to work with different people. Try to create activities that build on strengths, to show students how each person has something unique to contribute. Incorporate responsible technology use. Teach tolerance and respect for

1. Introduction Staff have a crucial role to play in shaping the lives of young people. They have a unique opportunity to interact with children and young people in ways that are both affirming and inspiring. This guidance has been produced to help staff establish the safest possible learning and working environments. The aims are to safeguard young people and reduce the risk of staff being falsely accused of improper or unprofessional conduct.

2. As a result of their knowledge, position and/or the authority invested in their role, all adults working with children and young people in education settings are in positions of trust in relation to the young people in their care. A relationship between a member of staff and a pupil cannot be a relationship between equals. There is potential for exploitation and harm of vulnerable young people and staff have a responsibility to ensure that an unequal balance of power is not used for personal advantage or gratification. Wherever possible, staff should avoid behaviour, which might be misinterpreted by others, and report and record any incident with this potential. Where a person aged 18 or over is in a position of trust with a child under 18, it is an offence for that person to engage in sexual activity with or in the presence of that child, or to cause or incite that that child to engage in or watch sexual activity

3. Confidentiality Members of staff may have access to confidential information about pupils in order to undertake their every day responsibilities. In some circumstances staf may be given additional highly sensitive or private information. They should never use confidential or personal information about a pupil or her/his family for their own, or others' advantage (including that of partners, friends, relatives or other organisations). Information must never be used to intimidate, humiliate, or embarrass the pupil. Confidential information about a child or young person should never be used casually i conversation or shared with any person other than on a need to know basis. In circumstances where the child's identity does not need to be disclosed the information should be used anonymously. There are some circumstances in which a member of staf may be expected to share information about a child, for example when abuse is allege or suspected. In such cases, individuals have a duty to pass information on without dela but only to those with designated child protection responsibilities. If a member of staff i in any doubt about whether to share information or keep it confidential he or she shoul seek guidance from a senior member of staff. Any media or legal enquiries should be passed to senior management.

4. Dress and Appearance A person's dress and appearance are matters of personal choice and self-expression. However staff should consider the manne of dress and appearance appropriate to their professional role which may be different to that adopted in their personal life. Staff should ensure they are dressed decently, safely and appropriately for the tasks they undertake. Those who dress or appear in a manner which could be considered as inappropriate could render themselves vulnerable to criticism or allegation.

Cyberbullying

Social media and text messages are vital to many students' social lives. Students use them to make weekend plans, support one another after a breakup, or commiserate about that difficult test. But sometimes students cross the line and use technology to bully or harass other students. We've all heard the stories about victims of cyberbullying — some choose to change schools and some even commit suicide.

The best approach to protecting students against cyberbullying is to be proactive and create guidelines before problems arise. Schools should create a policy that deals with cyberbullying that happens outside of school and then ensure students know that they can be punished.

What can you do?

- Get students involved. Seek out student input when the school is creating or updating guidelines about technology use. They know how their peers are using — and abusing — technology. Students are more likely to follow rules, and encourage others to follow them, when they feel ownership of the process. Further, you can check in with students to see whether the guidelines are effective and to learn when there are new issues that need addressing.
- Create a school mission statement or student bill of rights. A bill of rights sets positive expectations for the school. It could guarantee that students are able to learn in a safe environment and that they are treated with respect.
- Use technology to help. The KnowBullying app provides warning signs of bullying and tips to prevent it. It also offers conversation starters to help educators and parents connect with kids. Yik Yak, the anonymous messaging app that has become popular on college campuses, has been setting up geofencing to prevent messages at middle schools and high schools. Download the app, and check that your school is protected.
- Make sure your school has a reporting system that is easy for witnesses and victims to use. Provide a simple way for parents and students to report cyberbullying and other problems without fear of retaliation.

PEDOPORNOGRAPHY

Pedopornography often becomes an issue for schools when a dating couple breaks up, and one of the spurned teens passes along an old sext to other students. A lot of middle school and high school students are pedopornography, and schools and state governments are still figuring out how to handle this. In some states, pedopornography is prosecuted as a felony, with the same level of punishments as possessing child pornography.

While pedopornography might seem difficult to detect and stop, research suggests that adult intervention could change teen behavior. The most influential study on pedopornography was released in the journal Pediatrics in 2012. Of the students surveyed, 28% said they had sent a naked photo through text or email, and 31% said they had asked someone to send a sext. Girls were far more likely to have been asked to send a sext, and nearly 60% of them said that they were very bothered by the request.

If you need more reason to actively discourage this behavior, a follow-up study showed that pedopornography was a gateway to riskier sexual behaviors. So, a student caught pedopornography may be starting on a path to more dangerous choices. You can help stop that.

What can you do?

- Check whether your school or district has a policy on pedopornography. If so, make sure that your students know the policy and that it is posted where they can read it. If not, ask that one be created.
- Inform students of your state's laws on pedopornography. In some places pedopornography is a felony, and convicted teens would have to register as sex offenders.
- Involve the whole school community. Use an email or newsletter to inform parents of policies related to pedopornography, and ask them to speak with their children about it. We know that teens are less likely to engage in risky behaviors when their parents engage in open dialogue with them. As a last resort, parents can have the cell phone carrier eliminate photo- and video-uploading for their child's phone. Teens will still be able to take photos and videos; they just won't be able to share them.
- Make sure your school has an easy-to-use reporting system. As with cyberbullying, students need to be able to report problems without fear that they will be embarrassed.

Inappropriate Content

Almost all schools use filters to deter kids from getting into trouble online, but plenty of kids might accidentally circumvent these filters. Okay, maybe it isn’t accidental. Regardless, have a plan for these incidents so that you remain unruffled.

What can you do?

- Provide students — and parents — with the rules. School computer policies should discuss inappropriate content, password security, and viruses and malware. Enforcing the rules becomes easier when you know that students are aware of them.
- Stay cool. Sometimes your students really might stumble upon inappropriate content online by accident. If this happens, tell them to immediately close their laptop, or turn off their computer, and step aside so that you can deal with the problem.

Now, Keep up

Teens turn to their friends for advice about digital life because they think their parents and teachers are clueless about technology. Talk to kids about which apps and platforms they are using. Do a bit of research to learn the potential hazards of each program. Then put that knowledge to use. Your school can prepare for quick intervention by creating a computer-use policy, and students who know the consequences of inappropriate behavior will be less likely to break the rules. Your newfound knowledge might even help you gain the confidence of your students. They’re more likely to seek your advice if you know that Facebook is so over.

How can I stay safe on Facebook and what safety resources are available to me?

Here are a few things you can do to stay safe on Facebook:
- Learn how to use Facebook's privacy shortcuts and settings to comfortably share and connect with others
- Learn how to recognize sensitive content and behavior and how to report it

Remember these simple rules about staying safe online:

1. Never share your password
2. Think before you post
3. Adjust your privacy settings and review them often
4. Only accept friend requests from people you know personally
5. Report things that look suspicious

Watch out for Phishing

Even the best spam filters can’t catch every malicious or unsolicited email.
- If you ever receive an email from a company with a link to login and verify personal information (credit card or banking information, SSNs, etc.) online, always look at the URL of the website you are on to be sure it belongs to the company that you are dealing with. The part just before the .com (or other extension) is most important. For example, if you are on Chase’s website, the URL should read www.chase.com. If you see anything like chase.onlinebank.com, chaseonlinebank.com, chase.banking.net, that means you are NOT on Chase Bank’s actual website, rather you are on a Phishing site – one that looks like Chase but is designed to steal your information.
- Watch for shortened URLs, and numbers, hyphens or special characters in a URL. Scammers manipulate URLs to trick users. Be wary of URL's posted in facebook and sent via email. Use a search engine to identify the actual URL.
- Be sure the site is secure - look for signs of an encrypted Web site, including sites beginning with https as well as a padlock icon in your browser status bar (the location of this icon will vary based on browser).
- Retype the URL – if you are unsure if the site is real, close the browser window, open a new one, and manually go to the company’s site.

Be wary of Internet downloads

- Streaming media Web sites might seem harmless, but watching or listening to streaming media may mean downloading a special media player that could contain malware
- Downloaded files like software or other media can hide malware on your computer without your knowledge
- If a download seems too good to be true, it probably is—don't risk it!
- Never blindly accept a security dialog or execute an unexpected file, even if it comes from a web site that you visit often. Even the largest web sites can be compromised to include malware downloads and other security risks. Always carefully read and evaluate the provided text before making a decision. When in doubt - deny or cancel.

Watch out for spyware links

Any link promising to solve problems or make your computer faster for free, is most likely spyware

Don't just rely on your browser & antivirus software

- Don't rely on your browser and antivirus software to protect you from malicious websites. Browsers only warn you about sites but cannot stop you from going there. Even if you have high security settings and anti-virus software, visiting a risky web site can result in viruses, spyware or worse.

Beware of windows or pages that prompt you to click a link to run software

- Malicious web sites can create prompts that look like messages from your browser or computer. If you see a pop-up you think is risky, go to the company's web site for scans and downloads.

Don't provide personal information to get something free online

- Criminals may use this data to break into personal or work accounts.

Scrutinize search engine links

- When you use a search engine be very careful of the result you click on. Hackers use legitimate looking topics to trick you into clicking. Scrutinize the URL to ensure you are going to a legitimate web site.

Never trust free content

- Free movie, music and video downloads often include pirated content and just as often this content contains viruses and malware.

Vary your passwords from site to site

- When you use the same password across many sites it makes it easy for criminals to hack all of your accounts. Use more complex and varied passwords for sites with personal information such as banking sites.
- Use a secure program to manage passwords

20 ways to keep your internet identity safe from hackers

TWENTY COMMANDMENTS: THE DOS AND DON'TS OF ONLINE SAFETY IF YPU ARE AN ICT ADDICT

1. Never click on a link you did not expect to receive

The golden rule. The main way criminals infect PCs with malware is by luring users to click on a link or open an attachment. "Sometimes phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sidaway of Integralis. "However, targeted attacks and well-executed mass mailings can be almost indistinguishable [from genuine emails]." Social media has helped criminals profile individuals, allowing them to be much more easily targeted, he adds. "They can see what you're interested in or what you [post] about and send you crafted messages, inviting you to click on something. Don't."

Advertisement

2. Use different passwords on different sites

With individuals typically having anything up to 100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, first pets or favourite sports teams. Indeed, research by Ofcom last month revealed that over half of UK adults (55%) use the same passwords for most, if not all, websites they visit, while one in four (26%) use birthdays or names as passwords. Any word found in the dictionary is easily crackable. Instead, says Sian John, online security consultant at Symantec, have one memorable phrase or a line from a favourite song or poem. For example: "The Observer is a Sunday newspaper" becomes "toiasn". Add numerals and a special character thus: "T0!asn". Now for every site you log on to, add the first and last letter of that site to the start and end of the phrase, so the password for Amazon would be "AT0!asnn". At first glance, unguessable. But for you, still memorable."

• 3. Never reuse your main email password

A hacker who has cracked your main email password has the keys to your [virtual] kingdom. Passwords from the other sites you visit can be reset via your main email account. A criminal can trawl through your emails and find a treasure trove of personal data: from banking to passport details, including your date of birth, all of which enables ID fraud. Identity theft is estimated to cost the UK almost £2bn a year.

• 4. Use anti-virus software

German security institute AV-Test found that in 2010 there were 49m new strains of malware, meaning that anti-virus software manufacturers are engaged in constant game of "whack-a-mole". Sometimes their reaction times are slow – US security firm Imperva tested 40 anti-virus packages and found that the initial detection rate of a new virus was only 5%. Much like flu viruses and vaccine design, it takes the software designers a while to catch up with the hackers. Last year AV-Test published the results of a 22-month study of 27 different anti-virus suites and top-scoring packages were Bitdefender, Kaspersky and F-Secure. Meanwhile, security expert Brian Krebs published the results of a study of 42 packages which showed on average a 25% detection rate of malware – so they are not the entire answer, just a useful part of it.

• Advertisement

• 5. If in doubt, block

Just say no to social media invitations (such as Facebook-friend or LinkedIn connection requests) from people you don't know. It's the cyber equivalent of inviting the twitchy guy who looks at you at the bus stop into your home.

- 6. Think before you tweet and how you share information
- Again, the principal risk is ID fraud. Trawling for personal details is the modern day equivalent of "dumpster-diving", in which strong-stomached thieves would trawl through bins searching for personal documents, says Symantec's John. "Many of the same people who have learned to shred documents like bank statements will happily post the same information on social media. Once that information is out there, you don't necessarily have control of how other people use it." She suggests a basic rule: "If you aren't willing to stand at Hyde Park Corner and say it, don't put it on social media."
- 7. If you have a "wipe your phone" feature, you should set it up

Features such as Find My iPhone, Android Lost or BlackBerry Protect allow you to remotely to erase all your personal data, should your device be lost or stolen. "Absolutely, set it up," advises Derek Halliday of mobile security specialist Lookout. "In the case where your phone is gone for good, having a wipe feature can protect your information from falling into the wrong hands. Even if you didn't have the foresight to sign up, many wipe your phone features can be implemented after the fact."

- 8. Only shop online on secure sites

Before entering your card details, always ensure that the locked padlock or unbroken key symbol is showing in your browser, cautions industry advisory body Financial Fraud Action UK. Additionally the beginning of the online retailer's internet address will change from "http" to "https" to indicate a connection is secure. Be wary of sites that change back to http once you've logged on.

- 9. Don't assume banks will pay you back
- Banks must refund a customer if he or she has been the victim of fraud, unless they can prove that the customer has acted "fraudulently" or been "grossly negligent". Yet as with any case of fraud, the matter is always determined on an individual basis. "Anecdotally, a customer who has been a victim of a phishing scam by unwittingly providing a fraudster with their account details and passwords only to be later defrauded could be refunded," explains Michelle Whiteman, spokesperson for the Payments Council, an industry body. "However, were they to fall victim to the same fraud in the future, after their bank had educated them about how to stay safe, it is possible a subsequent refund won't be so straightforward. Under payment services regulations, the onus is on the payment-service provider to prove that the customer was negligent, not vice versa. Credit card protection is provided under the Consumer Credit Act and offers similar protection."
- Advertisement
- 10. Ignore pop-ups

Pop-ups can contain malicious software which can trick a user into verifying something. "[But if and when you do], a download will be performed in the background, which will install malware," says Sidaway. "This is known as a drive-by download. Always ignore pop-ups offering things like site surveys on e-commerce sites, as they are sometimes where the malcode is."

- 11. Be wary of public Wi-Fi

Most Wi-Fi hotspots do not encrypt information and once a piece of data leaves your device headed for a web destination, it is "in the clear" as it transfers through the air on the wireless network, says Symantec's Sian John. "That means any 'packet sniffer' [a program which can intercept data] or malicious individual who is sitting in a public destination with a piece of software that searches for data being transferred on a Wi-Fi network can intercept your unencrypted data. If you choose to bank online on public Wi-Fi, that's very sensitive data you are transferring. We advise either using encryption [software], or only using public Wi-Fi for data which you're happy to be public – and that shouldn't include social network passwords."

- 12. Run more than one email account
- Thinking about having one for your bank and other financial accounts, another for shopping and one for social networks. If one account is hacked, you won't find everything compromised. And it helps you spot phishing emails, because if an email appears in your shopping account purporting to come from your bank, for example, you'll immediately know it's a fake.
- 13. Macs are as vulnerable as PCs

Make no mistake, your shiny new MacBook Air can be attacked too. It's true that Macs used to be less of a target, simply because criminals used to go after the largest number of users – ie Windows – but this is changing. "Apple and Microsoft have both added a number of security features which have significantly increased the effectiveness of security on their software," says Sidaway, "but determined attackers are still able to find new ways to exploit users on almost any platform."

- Advertisement
- 14. Don't store your card details on websites

Err on the side of caution when asked if you want to store your credit card details for future use. Mass data security breaches (where credit card details are stolen en masse) aren't common, but why take the risk? The extra 90 seconds it takes to key in your details each time is a small price to pay.

- 15. Add a DNS service to protect other devices
- A DNS or domain name system service converts a web address (a series of letters) into a machine-readable IP address (a series of numbers). You're probably using your ISP's DNS service by default, but you can opt to subscribe to a service such as OpenDNS or Norton ConnectSafe, which redirect you if you attempt to access a malicious site, says Sian John. "This is helpful for providing some security (and parental control) across all the devices in your home including tablets, TVs and games consoles that do not support security software. But they shouldn't be relied upon as the only line of defence, as they can easily be bypassed."

- 16. Enable two-step verification

If your email or cloud service offers it – Gmail, Dropbox, Apple and Facebook do – take the trouble to set this up. In addition to entering your password, you are also asked to enter a verification code sent via SMS to your phone. In the case of Gmail you only have to enter a fresh code every 30 days or when you log on from a different computer or device. So a hacker might crack your password, but without the unique and temporary verification code should not be able to access your account.

- 17. Lock your phone and tablet devices

Keep it locked, just as you would your front door. Keying in a password or code 40-plus times a day might seem like a hassle but, says Lookout's Derek Halliday, "It's your first line of defence." Next-generation devices, however, are set to employ fingerprint scanning technology as additional security.

- 18. Be careful on auction sites

On these sites in particular, says Symantec's Sian John, exercise vigilance. "Check the seller feedback and if a deal looks too good then it may well be," she says. "Keep your online payment accounts secure by regularly changing your passwords, checking the bank account to which it is linked and consider having a separate bank account or credit card for use on them, to limit any potential fraud still further."

- 19. Lock down your Facebook account

•

- Facebook regularly updates its timeline and privacy settings, so it is wise to monitor your profile, particularly if the design of Facebook has changed. Firstly, in the privacy settings menu, under "who can see my stuff?" change this to "friends" (be warned: setting this to "friends of friends" means that, according to one Pew study, on average you are sharing information with 156,569 people). Also in privacy, setting "limit old posts" applies friends-only sharing to past as well as future posts. Thirdly, disable the ability of other search engines to link to your timeline.
- Advertisement
- You should also review the activity log, which shows your entire history of posts and allows you to check who can see them. Similarly, you should look at your photo albums and check you're happy with the sharing settings for each album. In the future you may want to consider building "lists" – subsets of friends, such as close friends and family, who you might want to share toddler photographs with, rather than every Tom, Dick and Harriet.
- Also, remove your home address, phone number, date of birth and any other information that could used to fake your identity. Similarly you might want to delete or edit your "likes" and "groups" – the more hackers know about you, the more convincing a phishing email they can spam you with. Facebook apps often share your data, so delete any you don't use or don't remember installing. Finally, use the "view as" tool to check what the public or even a particular individual can see on your profile, continue to "edit" and adjust to taste. If this all sounds rather tedious, you just might prefer to permanently delete your account.

- 20. Remember you're human after all

While much of the above are technical solutions to prevent you being hacked and scammed, hacking done well is really the skill of tricking human beings, not computers, by preying on their gullibility, taking advantage of our trust, greed or altruistic impulses.

1. Resources used
2. www.privacy.mk
3. www.bezbednonainternetorg.mk
4. www.nemrazi.mkwww.metamorphosos.org.mk

- https://chrome.google.com/webstore/detail/tinyfilter-reliable-conte/nlfgnnlnfbpcammlnibfkplpnbbbdeli?hl=en

1. : http://www.cyberpatrol.com/

- http://www.kidzui.com/

1. www.swgfl.org.uk