CYBER SECURITY. ARE WE READY TO USE MODERN, AND MOBILE TECHNOLOGIES? IF WE DON’T TEACH THE STUDENTS HOW TO PROTECT THEIR PRIVACY AND PERSONAL INFORMATION, WHO WILL?

J. Kucerik
iSkolstvi (CZECH REPUBLIC)

Abstract

Cyber security comes first before booting up our computer, turning on our tablet or smart phone. We have come a long way from using computers in the schools as a tool for education to using mobile devices, that are with us 24/7. Almost every student has a smartphone or a tablet. Mobile devices we entrust with most of our secrets, and private information. We share with our “digital friend” more information, and details from our privacy than we do with our family. Where did this trust come from? As humans we learn throughout our lives who to trust and who not to. It takes a long time for most of us to build such a trust worthy relationship with any one, yet we seem to not have a problem to unbox new phone or tablet and within a day entrust it with all our secrets.

As we do in our lives, we shall work on trustworthy “relationship” with new, modern and mobile technologies. We shall start with the teachers and then their students in elementary school on this subject and show them the way. Don’t expect their parents to do this as they are struggling themselves with modern technologies. It must be the school.

In this article we shall focus on fundamental basics such as possible risks involved using mobile technologies and how to prevent them. How to prevent losing our personal information, and data we don’t intent to share with others.

We will address the need of using passcodes and password. We all know we shall do that, but how do we really handle this subject? Many of us use mobiles without passcode. We use the same login and password credentials to many online services and social sites. Why do this? Simple, we don’t want anything difficult in our lives, so we use passwords that contains mostly our kids, pets name and we just add some memorable digits into it. Now living in digital world, it won’t hold anymore. We will focus on simple tools and how to adopt them.

Mobile technologies without an access to internet won’t just work most of the time. So here we are in the coffee, airport, library, shopping mall and we access either free WiFi, or we gain access code from waiters to their Wi-Fi connection. Now we are online, and we browse the internet, log in to different sites and medias. It takes only 15 years old sitting in the same coffee shop as you connected on the same Wi-Fi and having a free app on his computer to access all your data’s being transmitted online. Sounds easy? Unfortunately, it is. We will focus on tools to prevent that from happening.

Cyber security is a subject, that starts in school. Starts in your class before the tablet or phone goes on. We will go through our study and findings concluded in our courses for teachers in Czech Republic focused on cyber security. We will explain the way we have approached the subject of cyber security for schools and how to adopt it to become native for all users. We will focus on key elements of this issue based on user friendly experience at minimum cost.

1 INTRODUCTION

One of the most common cyber security threats are password thefts, public Wi-Fi, and applications that spy on us within them mobile devices. We will focus on possible threat scenarios, and the need for educating teachers at school and finally applying their new knowledge at the class and school curriculum.

iSkolstvi.cz is modern technology education company working both private and school sectors. In school sector we focus on educating teachers to use modern technologies such as tablets and how to use them in the classroom for education. Working with the technology itself and applications for education is enabling the teachers to present the students the learning subject in different and mostly more efficient way. Yet we see no education in cyber security. There are no classes with such subject as cyber security.
involved in elementary schools, and that generates a future problem not only for teachers, that are new
to these technologies, but also to the students, that are using the mobile devices both for personal and
educational purposes. Students start using them without appropriate knowledge of possible damage
that cyber attacks could do to them.

According to our own survey among 15 schools and total of 170 teachers in the Czech republic, 82% of
respondents place greater importance on having passwords that are easy to remember, and 89% write
their passwords down on a piece of paper. 83% of respondents said they use the same password for
multiple sites and services.

93% of respondents didn’t know, that connecting to a public Wi-Fi even password protected, may involve
potential risk of losing private data and passwords.

92% of respondents install applications to their personal and school mobile devices aps without prior
check of their possible security damage.

The survey was conducted from September to December 2018 in schools where iSkolstvi.cz lectures
the use of mobile devices in the class for educational purposes. In the beginning of each new course
section in new school we started our lecture handing out papers with surveys to fill out. The survey was
conducted anonymously so the final results would be as accurate as possible.

The results of the survey clearly indicate that using mobile devices as an educational tool is not the
problem. The biggest problem is the security and possible data loss prevention and lack of information.
Based upon this finding, we cannot expect the teachers to teach the students how to behave securely
while using the mobile devices.

Having the data from our study we have implemented in our lecturing courses cyber security for teachers
and place them first, before we proceed with any further engagement with the mobile devices. We have
created a list of most common threats and created 16hour classes for teachers to adopt user friendly
scenarios and best practice on cyber security issues.

Cyber security shall be thought at school hand in hand with the first use of any PC and/or mobile portable
technology. It is the tablet, mobile phone or just a regular PC user, that is most vulnerable and very easy
to attack and gain access to once personal information and data. The rapidly changing technology and
portability of mobile devices have changed people’s habits on how they use and rely on such
technologies. With technology increase of its functionalities, mobile devices carry out a many of our day-
to-day activities, such as web surfing, hotel bookings, setting up reminders, sharing files, instant
messaging, video calling, and even mobile banking.

Given all the possibilities and functionalities of mobile devices, these technologies are vulnerable to
online threats and to physical attacks. Some of the most common and dangerous security threats involve
malware, worms, spyware, phishing, and unauthorized access.

Since we were kids, we have learned to brush our teeth twice a day to prevent the plaque and possible
disease it may cause to our health. In today’s world of new portable technologies, we shall learn the
same practice and habits of such prevention and adopt the very basics on preventing our privacy against
any possible attack, that may cause us both personal and financial difficulty.

These basic skills shall be adopted in the school curriculum whenever portable and mobile technology
is being used for education purposes. Teachers should learn about possible cyber threats and how to
prevent them. This set of skills shall be adopted prior any devices and technology is being used in the
class for educational purposes. Finally, teachers shall engage students to learn these basics of cyber
security.

2 METHODOLOGY

From our study, we have identified following threats to focus on and to address:

- Password theft [1]
- Public Wi-Fi usage [2]
- Applications for mobile devices [3]

In order to properly address each issue and threat we must visualize the possible scenarios and
outcomes. We have implemented in our courses case studies that we have experienced with our own
customers from private sector. On these findings and studies, we explain possible scenarios, on how each threat was carried, and what was the outcome.

Finally, we have included in our course sets of solutions for each issue we need to address. There are many solutions that may solve each issue, yet we needed to focus on those, that are easy to use, user friendly, and also economically accessible for schools and teachers. Financial part of the solution is the trickiest one, as schools in the Czech republic do not have the same financial possibilities as private sector companies. We had to focus on solutions, that will fit to low cost budget criteria, will be still secure and reliable, and most of all user friendly. User friendly is one of the most important. From our findings from private sector, most users will not comply with new technology or application if it is too difficult to use, or if it takes the user too much time to work with on simple task

2.1 Password theft

This is one of the most common threat we deal with as users on daily bases. The danger is hidden while hackers access our password and use it to misuse our accounts. According to our study we have most of our users using same password for most of the internet sites, social media and services they use to access with their mobile devices. Users' passwords are mostly weak and their structure according to our study was mostly part of the name (kids, pets, etc.) and few digits containing date of birth of their kids. Weak passwords are easy remember and users don’t need to write them down. Strong passwords when used must be on the other hand kept anywhere to have them handy. Most of the time they are on paper in the wallet, stacked to a computer screen or written in digital notes. Those are the most used cases of our conducted study and as such we find them very weak and dangerous.

Case study of password theft:

User using the same password to most of the internet access, social media and services have got his password stolen by filling up a form when signing for new video streaming service. The video streaming site had user to fill out user form choosing user name and password. The site had only few videos for the users, even they presented a vast library of streaming. The offer was one month for free so as a user he did not expect any financial damage. Yet the main goal of this site was to access users name and password so they can finally use these credentials throughout the entire web using bots and humans to try to access with them other both free and paid services of this users. They have accessed users other accounts even social media and started to campaign their offers throughout the user’s identity and account. User have never got back his Instagram and Facebook access. Worst they have accessed users travel account in his company and booked through his identity several hotels and plain tickets. As the bookings were paid by user’s company, no one found out until after one month when users travel itinerary didn’t match the company billing. The damage was worth of EUR 3500 and the company insists on user to pay the amount, as they have investigated the breach and it showed it was due to stolen password and circumstances that led to this.

How to handle passwords

Easy methodology on how to think about creating passwords: Safest passwords is the one that even the user cannot remember for its difficulty. Each service, website or social media user registers at, shall have unique password. Best of all such password shall be long enough to be difficult containing small and capital letters, numbers and special character. Once in a while we recommend changing the password for each service. The period shall not be longer than 4 months. All passwords shall be securely stored and ready for the user when needed.

Solution:

There are many password manager providers that can handle all the required tasks. Password managers usually work across multiple devices and can be accessed on PC, mobile and tablets. They can generate strong user's passwords, store them securely and have them ready for the user when needed. Choosing the provider is the most important decision. In our research and recommendations received from IT engineers from Apple and Microsoft, we have implemented solutions:

- LastPass.com
- Avast.com
- 1password.com
Conclusion: We are working in our course with teachers to install one of these apps, set it up, and try to use. It is imperative that we go all the ways step by step with the teachers so they understand how it works and what it can do for them when needed. We have helped them to create accounts, generate some few passwords for their services, and teach them how to access them easily when needed.

2.2 Public Wi-Fi

This threat is not so much known and is not as often carried out by hackers as regular password thefts. Yet it may be even more dangers then simple password and identity theft. From our customer experience in private sector the threats are now being carried out in bigger cities. We anticipate this threat to spread further as it is very easy to carry out with minimum requirement on software and cost. We all tent to access a Wi-Fi wherever we go. Library, shopping mall, airport or coffee place. Some public networks are free to access without the need of password, some are accessible without one. Public Wi-Fi possesses a threat to all users that are connected into it if there is a hacker on the same Wi-Fi connected. To carry an attack for a hacker is very easy and it doesn't make any difference if the Wi-Fi is password protected or not. The hacker has the same password as the users and is connected on the Wi-Fi like everyone else. Public Wi-Fi is a security danger to users if they use internet without security protection. One of this basic security protection for transmitting data in public Wi-Fi places is VPN (Virtual Private Network). Imagine using your laptop, mobile or tablet in cafe place as a smoking area where each smoker generates cloud of smoke. Such “smoke” is being generated when transmitting any data when using Wi-Fi. It is invisible and we call them pockets. These pockets travel within the range of Wi-Fi similar like smoking cloud only invisible. These pockets represent data that you are receiving from internet while surfing the net and also when you type anything in the web. Anyone who has a low-cost computer and free software called Shark (there are many and more sophisticated) can collect these data and make sense of them in terms of uncover your user name and password, receive your photo or message you are sending to someone or downloading. This software pics up everything from that “cloud of smoke” and sends it to hacker’s computer. In this case you may not only lose your user name and password, but also your credit card information and private data. Now it is important to say, that not all of user’s data can be picked up so easily. It is based on the website you are visiting and the website security. Yet as a regular user you have no way of telling how secure that site you are on is.

Case study: This case study was performed by iSkolstvi.cz in closed coffee place with 5 users, that were aware of the study. We have run free Shark software on notebook worth EUR 200, and let it run for one hour. We have the users to browse sites of their choosing for news, shopping etc.. We had them to shop for vacation and also clothing online. For vacation we have used sites Fisher.cz and BlueStyle.cz. Fisher.cz proved to me secure enough so the users didn’t need to have own protection. Yet BlueStyle.cz was not secured, and we have accessed all information the users typed in the web including names, addresses, date of birth, user name, passwords. For shopping we had the users to shop for digital accessories. We had them to log in to Amazon.de and Insta360.com Amazon proved to be secured enough and we didn’t transmit any data. Insta360.com selling one of the world’s top 3D consumer camera proved to be weak. We have gained not only all users data, but also the entire credit card information. Most importantly regular users would have had no idea about us gathering their information, and wouldn’t know, that their all information and identity including credit card was stolen.

Solution: For user it is difficult to identify this public Wi-Fi access threat. There is one basic tool, that can prevent most common threat on public Wi-Fi called VPN. By installing VPN application, the user creates secure “tunnel” between the device and the intended server that hosts the website, online shop or any other service. VPN prevents the generate “smoke cloud” while on the public Wi-Fi and makes it much difficult to hackers to gain access to user’s data. There are many VPN providers and once again we have reached out to IT professionals from Apple and Microsoft for advice, on which solution to use. We focused on secure, easy to use and minimum cost solutions:

- Avast.com (SecureMe and SecureLine)
- NordVPN.com
Conclusion:

We have adopted the implementation and use of VPN in our courses. Each of our regular course starts with teachers to check their VPN to be running and after that they get password access to our Wi-Fi connection. We believe this practice creates a habit to start with on this particular issue.

2.3 Applications for mobile devices

Like Steve Jobs once said: “We have an app for that.” Tablets and mobile devices would be worthless without applications. We use them for pleasure, entertainment and work. We tent to download and install applications as we see fit and also because most of them are either for free or at minimum cost. Unfortunately, not every app developer’s intention is to bring the user comfort. There are some apps, that contain threats in terms of spyware and viruses. Once again for regular user it is very difficult not even impossible to say to identify such a faulty application. They often pretend to be a game, or QR scanner. Yet they also may have spying software that sends users data from the device to the hacker without the knowledge of the user. It is rather difficult to properly address this issue to general population. Such threat is unfortunately very real and happens on daily bases to millions of users. The spyware collects private information stored in the device including names, address, credit cards and others.

Case study:

In October 2018 and February 2019 there were two major security hacks carried out in Czech republic focused on users bank account access from mobile phones and tablet devices. An application name Blockers call 2019 [4] and QRecorder [5] was downloaded by thousands of users in Czech republic. Blockers Call 2019 was supposed to get rid of unwelcomed incoming phone calls from marketing companies, and similar. QRecorder is an app that records a phone call conversation, which in some case may come handy. Both of the mentioned apps had installed software within, that focused on user’s access to a bank account from the device. The app obtained the users credentials and even SMS message sent from a bank to verify user access and money transfer. Both apps where capable of handling the users account and wire money. Thousands of users were affected in this case.

Solution:

As mention earlier there is no easy solution to this as the major problem comes from the app store provider. In cases of these threats it is unfortunately the Google Play store. As it is an official site for app purchases, users may get faulty impression, that everything they download from this store is safe and secure. As for Android users the only thinkable solution is to minimize the amount of application, purchase and download applications only from trust worthy developers (Microsoft, Google, Adobe, etc.) to simplify it shall be the company names, that are known for the work they do and their proof of reliability throughout the years. Android users shall most definitively use virus, spyware and worm protection from known sources and companies. For Apple and its iOS users, this type of threat is minimized to zero. There had not been a breach in terms of described case study so far. It is due to the hardware and software solution Apple provides, and mostly the way Apple controls all apps that initially places in the App Store. Both Android and Apple users are recommended no to download the applications from any other source, then their official stores.

Conclusion:

We do recommend our clients in school to use iOS devices from Apple. As in this initial and very important decision on which technology to use may and will ensure further elements of security.

3 RESULTS

Based on our study in 2018 we started to work with our new course for teachers to implement basic security habits for mobile technologies and tablets. We attend all of our schools that participated in our initial study, and currently we see the progress in adopting these cyber security skills. We see, that the easiest one and fast to adapt is applying VPN security to avoid the public Wi-Fi security thefts. Password protection is now at much higher level and use, yet it needs an improvement. At this point we don’t have official paper data to be precise. We plan to conduct another survey in the same schools in October 2019, to check the one-year progress in adopting the security measures and skills. So far, we see that more teachers are using password manager. The passwords they use became strong as they are being generated by the software itself, yet we don’t see much progress in changing the passwords after
4month period. Also, we have had encountered, that some users don’t use the password manager for all of their online access.

So far, we do see overall progress in terms of better identifying possible threats and adopting basic security measures. Those teachers that feel confident in their own use of technology, also started to share the best practice and information about the cyber security in their classes.

According to our findings, the key to adopting security measures and skills to our schools, we need to focus on user friendly and minimum cost solutions.

REFERENCES

[1] Avast, Check your e-mail for possible password thefts
URL https://www.avast.com/hackcheck

[2] Kaspersky, Public Wi-Fi threats
URL https://www.kaspersky.com/blog/secure-connection-android-ios/20255/

[3] Cnet, How to check dangerous apps for Android
https://www.cnet.com/how-to/how-to-check-your-android-phone-for-malicious-apps/

[4] Novinky.cz, Blockers Call 2019 article