User Ethics and cyber protection habits in relation to cyber security

Intro

There are two ways to interact with a particular system - conventional and unconventional. The conventional way is to interact, such as running your computer, logging in, waiting for the Windows system to load, open a file, for example, word, and use it to write something. This is because the Windows system has built-in security protection. It's unconventional to use another computer with another system, such as Linux, access to the other computer via Linux, and then access the selected file. Why with Linux though? The answer is very simple. The Windows access system fails to use Linux, which means we jump over the security and provide access to the Windows system, which we are not really entitled to. Moreover, this protection is set so we cannot access the file in question without getting into our account. However, if we try to access the file in Linux, we will succeed because the Linux system does not see and does not care about Windows protection. This unconventional way of interacting with the system is also called hacking. When it comes to cyber space, we are not talking about the machines, but about the people behind them. Machines are simply a tool in the hands of people and their behavior largely depends on our intentions. This report will be about the intentions of people as consumers both at work and outside, about their noble or malicious ideas and intentions.

Internet user ethics

The topic is related to the user habits in the internet which are related particularly to cyber security. The so-called Internet user ethics is based on a set of moral principles that govern an individual or a group on what is acceptable while using internet meaning one should respect the rights and property of others on the web(internet). Internet user ethics means acceptable behavior for using it.

First, and one of the most important thing is **acceptance**. We must accept that the Internet is not apart from the universal society but it's a primary component of it. We must accept that Internet is not a value free zone which means that World Wide Web is a place where all values are considered in the broadest sense, so we must take care while shaping content and services.

The second principal is the so-called **sensitivity to national and local cultures.** It cannot be subject to one set of values like a local newspaper or TV channel, and we have to accommodate multiplicity of usage. It belongs to all of us and there is no barrier of national and local cultures.

Using e-mail and chatting. Internet must be used, and it is used for communication with family and friends every single day by everyone of us. Its important to notice that we should not use it for chatting or communicating with strangers and should not forward e-mails from such people. There are risks in such action and we must teach our children on risks involved by chatting or forwarding e-mails to strangers.

Those strangers can also be **pretending to be someone else**. We must not use the internet to pretend as someone else and fool others. There are hundreds of thousands of people who are hiding their identity on the internet pretending to be someone else and most of the time they do it for reason particularly having access to your personal information. We must teach ourselves and our children that fooling others and hiding your own identity is a serious crime.

Hiding your personal information is a rule number one for safety both for you and your system. We should not give personal data like home address, phone numbers, interests, passwords to anyone. No photographs should be sent to strangers or apps because it might be misused and shared with others without your knowledge. As you know social media is using ads and apps to collect your data and despite of the rules and protections it can leak anywhere into the cyber space.

Internet is used to learn about everything – music, culture, videos, playing games etc. Often, we want those fails on our computers, to be **downloaded** and used for later. One of the internet user ethic principal is to respect the copyrighted materials of others. By downloading the copyrighted content to our PC, we can share it with someone else and that's a violation and can be considered a crime according to law. That's why we must not share downloaded or purchased copyrighted materials and that should be taught to our children and they must be aware about the importance of copyrights and issues of copyright.

Avoiding bad language. This is the common rule for the internet user ethics which is also the most violated. We must not use rude or bad language while using e-mail, chatting, blogging and social networking. We need to respect the point of view of others and should not criticize anyone on the internet and the same should be thought to children. There are thousands of reports for verbal harassment or hate speech via chatting, social networking and even online gaming. Most of the victims are teenagers.

Internet use (Cyber) ethics is a code of behavior for moral, legal and social issues on the Internet or cyber technology. This ethics also includes obeying laws that apply to the online behavior. By practicing it, we can have a safer and enjoyable experience on the WEB. Cyber bullying is the use of information technology to do harm or harass other people in deliberate manner.

In 1992 the Computer ethics institute introduced the "Ten commandments" for computer ethics to create a set of standards to guide and instruct people in the ethical use of computers and internet. Here they are:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Internet ethics means an acceptable behavior! We must respect the rights and property of the others on the web.

Cyber protection habits / Good security habits in the internet

Every week we face a new virus that is attacking computers all over the world. Phishing scams, malware, worms, trojan horses and spam continue to be everyday threats. The first line of protection is our security software updated to the latest version. Yet there are other things we can do to help protect ourselves. Things that should be second nature but end up being forgotten as we surf the WEB or rush to catch-up on e-mail. Those are the good computer and internet security habits that can go a long way to making sure we stay ahead in the constant battle to keep cyber-safe. Most common protection habits:

1. **Locking your computer when you are not using it.** Even if you are away from your computer for just a few moments, there is a chance your data could be compromised. For example, breaking your wi-fi network can be performed under 20 seconds. We better close our computers and make sure the screen is locked after going somewhere, even in the next room.
2. **Disconnect from the internet.** Most broadband connections allow us to stay permanently connected to the Internet, but this convenience comes with risks. The chances of your computer being attacked is much higher if you are always connected. This is particularly true if you are using your computer at home without an adequate firewall.
3. **Adjust your security settings.** The Windows and Mac OS operating systems all have multiple security settings, as do popular browsers like Chrome, Firefox, Safari and Internet Explorer. Make sure the settings are appropriate for your computer and are adjusted for each individual user.
4. **Check for security patches and software updates.** Microsoft and other popular operating systems offer regular updates and software patches to protect against viruses and security flaws. Make sure your computer regularly checks for updates or visit the appropriate web page to get the latest download.
5. **Change your passwords.** Change your passwords regularly, particularly for financially sensitive accounts and web sites. Don't use the same password for multiple accounts. Do not keep a copy of all your passwords on your computer. It will be much harder to re-create or access accounts if data is lost.
6. **Protect against power surges and outages.** Computers are easily damaged by power surges. Make sure you are protected and considered disconnecting your computer during thunderstorms.
7. **Back up your data.** Set aside a few minutes a week to back up your files and personal data. It can help you recover your files in case of data loss or virus attack.

Good security habits for everyone[1].

Recently one of the biggest antivirus companies in the world "KASPERSKY" decided to test the cyber-literacy levels of the internet users. They found out that the number of "literate" web users is surprisingly small. They performed an experiment with a phishing page. They gave four screenshots of Facebook homepage to choose the one they feel safe enough to log in.

[1] "Good security habits for everyone", Kaspersky LAB Daily

The result was that only 24% of the people picked the right one. The remaining 76% chose the phishing page and thus gave away they credentials to cybercriminals – and that was just one simple question. Of course, we should note that the ability to tell a genuine web page from a fake one or a legitimate email from a spam message is not the only criteria to define cyber-literacy. A cyber-literate user possesses a variety of good habits. For example, downloading unknown files from murky web pages is a bad habit, whereas checking the operating system for vulnerabilities and updating it regularly in order to repel viruses is a good habit.

A good habit is backing up your data, whereas disclosing too much information on social networks is a bad habit. Weak passwords are a bad habit and keeping them written on a piece of paper or a file in the PC, whereas installing new apps or software without a second thought, not even looking at their license agreements or access rights is even worse. Cyber-literacy is the basics of information security, which if followed, might protect your data, privacy, money or even your device. In a real world, we all follow the laws of self-preservation for example, you would not: end up in a ghetto in the dead of night; tell your credit card PIN code to anyone who happened to ask; or leave your key sticking out of the keyhole of your front door. Those habits are as natural as an ability to write or read, and, apart from some rare exceptions, the majority of people act out of instinct when making these security decisions. As we grow old this instinct of self-preservation develops and the carelessness seen in children fades away to be replaced with necessary caution. However, these instinct stops working for some reasons when you are on the Internet and many people become as careless as children, assured that nothing can go wrong. According to the security survey performed by “Kaspersky” only 50% of 18000 respondents chose a safer option and none of them reached the highest score on the test. The world of technology is evolving through tectonic changes and drastic shifts, which human awareness cannot keep up with. Someone still believes that cyber threats are fictional, someone is sure he can easily withstand them, and someone just lets it be.

Reality shows that threats are becoming increasingly abundant and sophisticated, so the odds of being lucky on the Internet are constantly declining. The cybercriminals know this and increasingly count on human nature: they place odds on people not doing something or not noticing something suspicious, ultimately delivering a fresh virus to their machines. So what can be done about it? We can provide a single answer for that: if you don’t sense the danger that does not mean there is no danger. Once you assume that a little more caution would not hurt, you might be spared many serious problems, like losing the only copy of your son’s childhood pictures, your unfinished novel leaking online or massive theft of your money from the bank account. And, as it goes without saying, one should use reliable software to protect all of your devices; your antivirus should be updated regularly and scan your files from time to time. Should it react violently on one of your programs, just trust it and don’t disable it just because it is annoying (as 19% of respondents do). Don’t make the lives of cybercriminals easier! In fact everyone can check their cyber habits and literacy in this quiz performed by “Kaspersky”.[2]

[2] Kaspersky LAB Daily, Cyber habits literacy Quiz: https://www.kaspersky.com/blog/cyber-savvy-quiz/

User threat recognition[3]

According to every statistic for cybersecurity in seems that the security industry is not catching enough bad guys. Majority of breaches are reported by external parties and law enforcement agencies after stolen assets shows up in the underground economy or elsewhere. These facts are pointing in the direction that we need to consider new ways of detecting breaches more quickly and on our own. Currently available cyber security tools are pretty good at detecting known attack patterns. If an attack matches a signature, talks to a known bad place, uses unencrypted protocols, or happens within the infrastructure that you closely monitor, you can reliably detect it as it occurs (if the technology is set up properly). What people struggle with is detecting unknown attack types, new malicious behaviors, and insider threats.

Security professionals also struggle with attackers hiding within a bell curve. Many attacks in the past occurred on a Friday just before the weekend, because there is plenty of time to break in, ransack the place, clean up, and install a back door for persistent access. Today, things have changed, and we now often see attacks on other days of the week gaining benefits during the peak hour of network traffic.

Many experts present the future of threat detection and analytics as **a river delta,** as analogous to the current enterprise security landscape. Endpoint and other security devices produce small streams of operational data. This data flows downstream, where it's aggregated into rivers of enterprise log and security data. The rivers include business operations context, IT operations logs, and information security events. When you aggregate and monitor these using real-time correlation in a security information and event management system, they anchor the modern cyber defense center, which monitors real-time correlated security events to detect indicators of potential attacks in progress. Given the modern threat landscape, you can now picture how real-time capability requires a correlation and longer-term analytical capability as a supplement. You need to expand operational post-hoc analytics to the data "ocean," by assigning this work to a newly formed "hunt team". There should be an important operational link between the hunt team and the cyber defense center, especially when an unknown attack takes place. Once an attack type is detected, it is then converted into automated (and hopefully) real-time detection, so in the future you can catch it in real time.

In terms of geography, the tactical technologies for breach detection and prevention are in the "streams" of data (e.g., intrusion prevention), operational monitoring capabilities sit across the rivers of data, and any strategic data analysis for breaches resides in the oceans of data. People and processes are a critical link between these levels.

The base detection technology commonly used today is **detect, explain, explore, understand** mechanism. **Detect –** this is the ability to highlight the events of interest in real-time. **Explain –** this often results in reporting which includes threat vulnerability, compliance reports etc. **Explore –** basically here we query data and produce small datasets on which we can conduct a basic, formal analysis. **Understand –** talking about understanding includes also the context. This is the most important component of the detection because it can be tricky to decide whether unusual activity is truly a breach or simply a benign event. Having context is critical

[3] Cybersecurity threat detection analytics, HPE Enterprise security team

in that decision. To gather context, we can collect information like assets, networks, identities that we are protecting. This will help to decide if the event is malicious and should be escalated as a breach or is simply a compliance scan. Becoming a professional in cyber security, particularly in threat recognition we have to catch the attacks earlier. This requires a guiding vision and a plan to build a system which will grow with your needs. Only then can you achieve reliable behavioral detection of advanced attacks and insider threats.

Users/Employees in SME's as potential cyber criminals.

Companies have come a long way in their ability to ward off internal and external cybersecurity threats. However, as the pace of technology innovation speeds up, the threat landscape companies face only becomes more complex. Guarding devices and online data is an ongoing (and always fluctuating) effort. By mid October 2015 there were 606 reported data breaches reported, compromising more than 175 million records. It's clear that businesses must make it a priority to protect their own, their customer's, and their employee's confidential information.

With what we said so far unfortunately worker/user cybersecurity knowledge and habits still lag behind. Despite some of the incidents come from organization's subpart planning and systems, most of them comes from simple employee error. Being aware of **IT** best practices, cybersecurity is reflected in the many technology decisions employee make daily, whether it's changing logins regularly, avoiding predictable passwords or dodging phishing attempts. Despite the widespread sentiment that end users are more tech savvy than ever before, the reckless behavior persists.

This stuff can be simply explained by an experiment performed in the past years.

The USB Drop experiment. Probably you all heard about this experiment. It is one of the most prominent cybersecurity incidents to draw attention to the perils of consumer technology in recent years. A social experiment performed by CompTIA from August to October to observe the cybersecurity habits of users – employees and consumers, when faced with found USB sticks. They dropped 200 unbranded USB sticks across high traffic public spaces – business districts, airports, coffee shops and public squares. Every USB had a text files prompting anyone who plugged the found USB in to e-mail a specific address or click through a trackable link. In a few weeks 17 % of the consumers and employees who picked up the found USB sticks, plugged it in their devices, opened the text file and either clicked the unique link or emailed the listed address. Among those 17% were a number of IT industry workers at the International Airport of San Francisco and a worker in a security office in a multinational corporation's office building. Some of those people who plugged in the USB emailed the alias address and even asked if the USB had a virus on it. Blindly trusting found USBs – or unprotected Wi-Fi networks, or emails from unidentified third parties – puts more than the individual at risk. As the findings show, even the most IT literate end users can make precarious decisions when faced with potentially suspicious technology, demonstrating how challenging it can be to instill strong cybersecurity habits (not merely knowledge). We can all make our conclusions from this experiment. As a remind the USB viruses were popularized by

“Stuxnet” – an infamous worm, which U.S and Israel used to infiltrate Iranian nuclear centrifuges in 2010. Remember USB sticks programmed with malware can quickly infect devices and critical infrastructure and can do unimaginable damage.

Even the most advanced IT infrastructure for detecting and eliminating cyber threats and attacks can be overcome. Sometimes the attack can last seconds and sometimes it can take years depending on what information you are seeking and how deep it is encrypted. For example, a modern virus will not be aggressive when it performs an attack for gathering certain data. It will execute a process which will search for that data only for a while, just enough not to be detected by the antivirus program or the user. It can stay like this for days, months, even years until the needed data is gathered.

Though employees are largely aware of the risks of poor cybersecurity habits, many don’t apply that knowledge. Workers’ overall IT behaviors, from Wi-Fi connectivity to online account maintenance, reflect a degree of vulnerability that malicious actors can easily exploit. Employees continue to connect their devices to unprotected Wi-Fi networks in spite of the inherent security risks. Almost all employees connect their laptop or mobile devices to public Wi-Fi networks, and some of them handles work-related data while doing so. Perhaps due to the lifelong ubiquity of technology for younger workers, the likelihood of connecting to unsecured wireless networks negatively correlates with age. If you have more than a couple of people at your business, you’ll need to control which employees have access to which systems and applications. You wouldn’t blindly give every employee a key to your safe, would you? Underpinning many of these findings is the reality that many employees don’t receive the training necessary to combat cyber risk. Most of the workers report that their organizations don’t provide any form of cybersecurity education or communicate specific end-user best practices. Organizations that have yet to incorporate IT security into their onboarding and professional development programs are increasingly vulnerable, given how many issue employees devices and entrust staff to handle sensitive corporate data.

Ladies and gentlemen, thank you for your attention.

Atanas Radev

Expert at Center for National Security and Defense Research at Bulgarian Academy of Sciences

radevatanas@yahoo.com