# Network Threats

Threats Of College Network Security

**Social engineering -** is a set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes.

**Example of threat:**

There are many threats to anything, but the main one will always be a careless and gullible person. Because someone on the street can tell her that he is from the college staff, even show her a badge, and say that she needs to come to the college, go there, do something. That is manipulation.

**Protection methods:** access levels for staff and all students, limited access to devices critical to the system, badge control and logging of all authorizations.

1. **Phishing -** attack in which the victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data.

**Example of threat:**

Another basic threat is phishing, which can be used to gain access to a member of staff who has access to a specific function of the college system. For example, someone from the IT department or the admissions office received an email saying that the site for working with the college platform has been updated, and to continue using it, you need to follow the link. A person enters without noticing anything, enters a login and password (possibly additional data) and receives a message about an unsuccessful login. Meanwhile, criminals go to the official platform, since they already have all the necessary data, and do what they need.

**Protection methods:**

access levels for staff and all students, limited access to devices critical to the system, limited access to critical platforms from outside the college network, 2-factor authentication, MFA, and the ability to lock/freeze the account until it is secure.

1. **DoS/DDoS -** a large number of requests to the server, which can crash the system, usually hackers use a botnet.

**Example of threat:**

If you limit the work of services that are critical for the college ecosystem, you can infect other less important devices, which will infect other devices of the ecosystem after all the servers are fixed.

Or it is quite a normal situation for small services, when some kind of opening is taking place, for example, the season of registration and submission of applications to college, or a site where the results of exams are displayed - a large number of users will log in at the same time, which will put a load on the server, and if the number of these users will be very large - prepare for server dumps.

That is, your system can be brought down even only by a large number of requests..

**Protection methods:**

Ray Limits, restricting resource use only to the college network, powerful servers, and good load balancing tools.

1. **Worms -** distribution of infected programs over the network, with the aim of infecting a larger number of devices/

**Example of threat:**

Your college most likely has devices for working with the system and learning, i.e. computers, and since there is direct access to them, an attacker can, for example, bring an infected flash drive and connect it to the computer, thus infecting it, and he already has his queue will crawl through the web and create many holes or backdoors for other malicious programs.

**Protection methods:**

Limited access to devices critical to the ecosystem, system restrictions on all devices, use of a firewall, antivirus, scanning of a flash drive before using a computer.

1. **Combined malware software.**

Usually, an attack on the ecosystem of any organisation is combined and planned. That is, only social engineering, or just a worm that infects the network, will not be used. Phishing, worms, Trojans, viruses, etc. will be used to get the maximum amount of useful information for attackers, and to disable everything that manages to infect after the work is finished. Combined viruses can include modules for tracking, infecting and cloning viruses on a PC, spreading them over the network.

**Someone’s social media profile being hacked and manipulated against the college:**

If, for example, the director's account was hacked, it already carries a great danger for this institution, because despite personal chats, this account can be used to manipulate other members of the institution, humiliate the institution, and many other things that can damage the reputation of this person, possibly even financially blackmail for the redemption of this account, etc.

**Why is it necessary for staff to protect themselves against social media problems – how will this reflect upon the college?**

It is definitely necessary, because if their access is compromised, it can have a very bad effect on the institution's reputation, the influence of manipulation and blackmail, or simply monitoring their account and life.

It can also give the establishment a negative reputation, as attackers can write something bad about it. Or, this account has been used to log into college platforms, meaning attackers can gain access to those platforms. Therefore, you should use work and personal accounts to separate personal life and work. At the same time, for a personal account, limit the number of people and access so that no intruder can track you.

**What are the dangers of careless uses of social media? (Derogatory posts about your boss etc.)**

If you write something bad about your boss, in public, or even for a limited number of people - there will be people who will show it to your boss (even anonymously), and it will already affect you, and it depends on the messages about the boss. If you wrote something very, very derogatory, he will most likely fire you for the article, and that stigma will remain when you try to go to other companies.

Information on the Internet spreads very quickly, so look carefully and think about what you post on the network.

**Who might monitor and why would they want to monitor someone's online presence?**

Criminals who can benefit from this, because this way they get more information about you, which can be used against you, for example for blackmail. From the photo on Instagram, you can understand where you have been, when you have been there, with whom you have been there, and the more such information you have, the easier it will be for criminals to manipulate you in the future.

Act’s explaining

* **Data Protection Act** - Any web service can use your personal data, but not always with malicious intent, this law obliges such companies to spend money and improve the security of this service so that a common hacker cannot get data from it.
* **Copyright and patent law** - It was invented so that someone else could not appropriate someone's achievements. That is, music always has an artist, and if he owns the copyright to this song, he can restrict its use in other people's videos on YouTube, for example. Or if someone developed a transparent display and patented such a technology. Someone else wanted to appropriate this technology and say that he invented it, but he will not be able to do it legally.
* **The computer misuse act** - hacking, unauthorised access and similar things that are illegal, that is, lead to breakdowns, leakage of information, infection of computers, spread of viruses - should be punished.
* **Freedom of information act** - any information that does not have problems with copyright, PC abuse, patents - can be illuminated and released on the Internet, regardless of its value.