



DIESEC™
A Brand of Dietzel & Company GmbH

DIESEC's CYBER SECURITY QUARTERLY REVIEW

[Q3 2020]

**Q3 Cyberattacks
and Trends: Social
Engineering Takes
the Upper Hand**

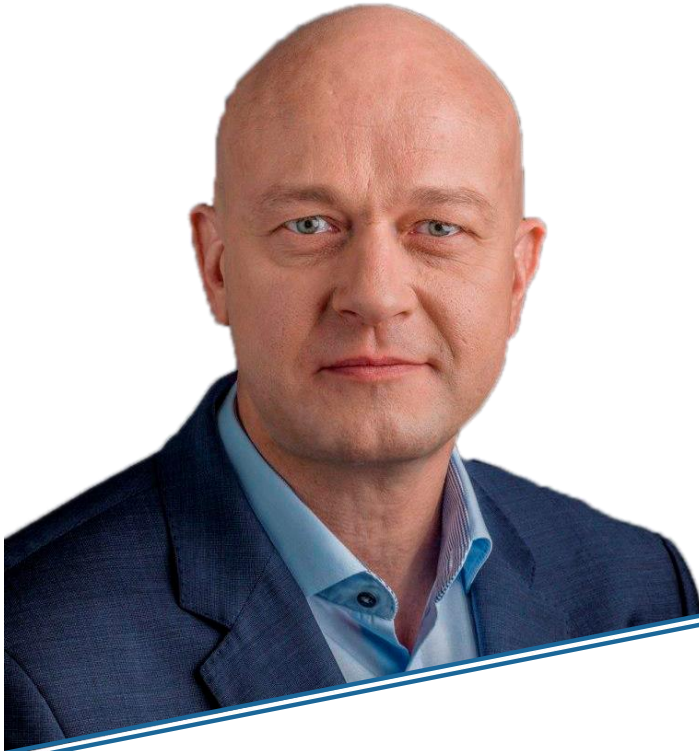
**How to Make Your
Cloud Hacker-proof**

**How to Avoid
Being Hacked Like
Twitter**

**Protect Your
Assets. Going
In-depth**

**What is
Coming Up?**

Dear readers,



I am glad to greet you on the pages of the first issue of DIESEC's Quarterly Review, a new tool that will help you to survive and prosper in today's full of danger cybersecurity world.

Why do we think this Review will be useful for you?

Almost 12 years DIESEC has been delivering the best cybersecurity services to hundreds of clients worldwide. Mostly, we deal with the clients for whom cybersecurity equals surviving in business: financial institutions. We provide them with a whole package of modern cybersecurity services, including

penetration testing, information security auditing, data protection, GRC (governance, risk management, compliance) staff education and digital forensics. Every day we face and successfully solve complicated cybersecurity challenges. We strive to contribute to the building of the cybersecure world as much as possible.

And recently we have concluded that we have even more to contribute. Nowadays, cybersecurity-relevant information and experience are at a premium. And sharing this experience, findings and other valuable information can be really helpful in creating cybersecurity protection.

Knowledge is power. In relation to the cybersecurity issues, knowledge often makes the difference between the life and death of a company or an organization. The ability to recognize what is going on with your digital assets can keep your business afloat, while unawareness can plummet it in no time.

That is why we decide to issue this Review to share the knowledge and experience gained by our experts during the years of working in the cybersecurity field. Sharing is caring.

The Review consists of the most significant cybersecurity topics of the last quarter to help you protect your assets in the best way possible.

Section 1, "Current Trends", includes the general analysis of cybersecurity attacks and incidents in the last quarter from the standpoint of the DIESEC's experts. You will find out what kinds of attacks and malware were used and discover the up-to-date trends of threats and risks to build the optimal defense line.

In **Section 2, "From DIESEC's experience"**, we will share our approaches and methods of solving current problems in the cybersecurity field. For example, in this issue you will learn how to correctly secure your cloud environment on an example of DIESEC's case: transferring a digital forensic lab in the cloud.

Section 3 is named "The Attack of the Quarter", and it is exactly what it sounds: It describes the most dangerous and sophisticated attack of the last quarter. In this issue, we will carefully analyze the infamous and stunning Twitter hack.

In **Section 4, "Protect Your Assets"** you will find our advice on methods and techniques to protect your assets from the attacks described in the current issue of the Review.

Finally, in **Section 5, "What is coming up?"** we will give our forecast about the main cybersecurity trends, threats and risks for the near future to make you better prepared for dealing with them and protect yourself.

Live informed and secure with DIESEC!

Sincerely yours,

Carl Dietzel,

DIESEC's founder and CEO

Contents

Section 1. Current Trends. Q3 Cyberattacks and Trends: Social Engineering Takes the Upper Hand	5
Hunting for easy preys	5
Cybercriminals on cloud nine	7
Phishing e-mails	8
Ransomware under COVID-19 influence	8
Mobile threats: FakeSpy uses fake post-services	10
The trend estimation	11
Section 2. From DIESEC's Experience. How to Make Your Cloud Hacker-proof	13
What you need to protect in the cloud	14
From Firewalls to Humans.....	16
The Secrets of Digital Forensics Implementation	17
Some Security Tips to Remember.....	19
How to implement cloud security in the best way	20
Section 3. The Attack of the Quarter. How to Avoid Being Hacked Like Twitter	21
The attack: Would you like to double your money?	21
The attackers: Exploiting human vulnerabilities.....	22
The method: from Slack to spear-phishing	23
Lessons to learn: Strengthen the human factor	24
How you can avoid falling prey like Twitter.....	25
Section 4. Protect Your Assets. Going In-depth	27
Vulnerable points.....	27
The ABC of Defense	28
Section 5. What is Coming Up?	30

Section 1. Current Trends. Q3

Cyberattacks and Trends: Social Engineering Takes the Upper Hand

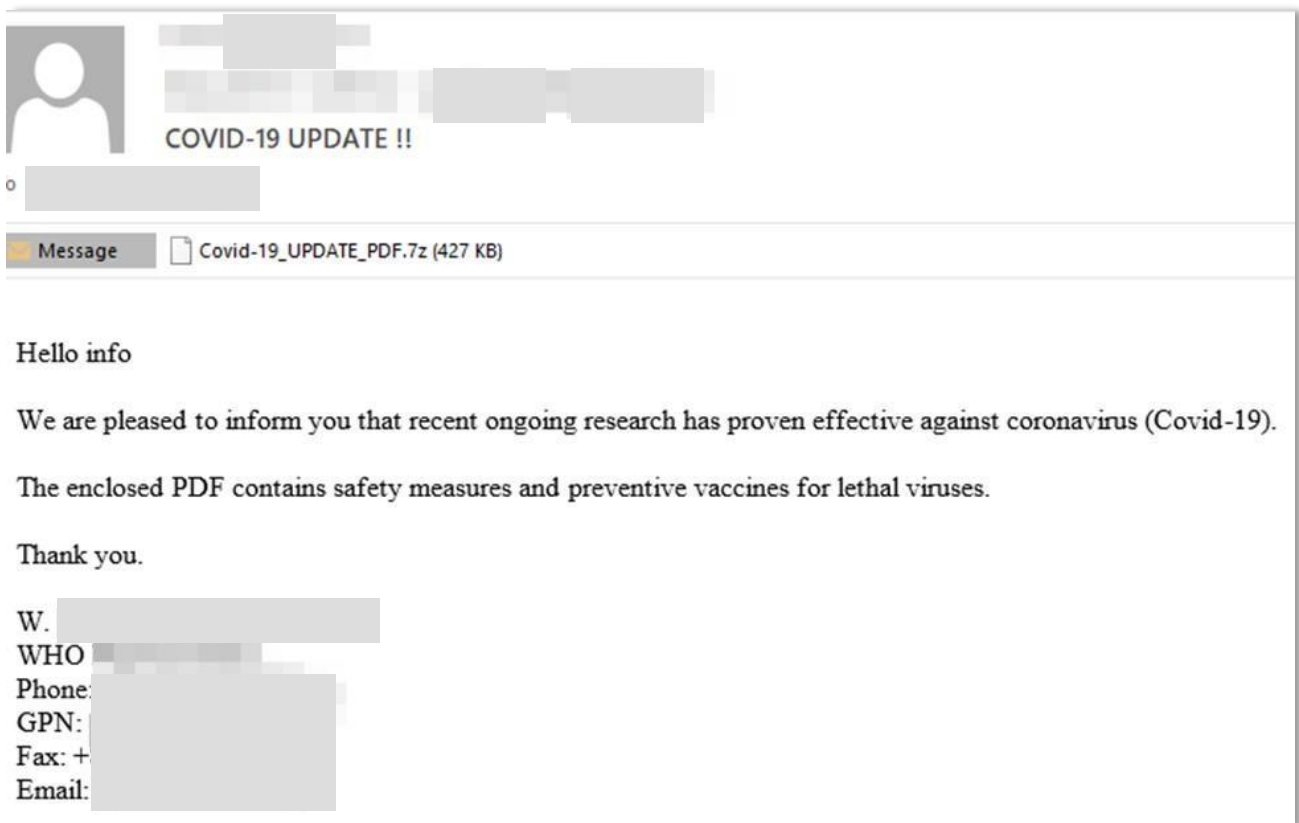
COVID-19 strikes almost everything in the world, and the cybersecurity field is not an exclusion. Observing the Q3 events and incidents makes obvious the fact that Coronavirus has cardinally changed the world's cybersecurity landscape and these changes look irreversible for the nearest future. More of that, these new trends seem to be able to distinguish the whole manner of the attackers around the world.

Hunting for easy preys

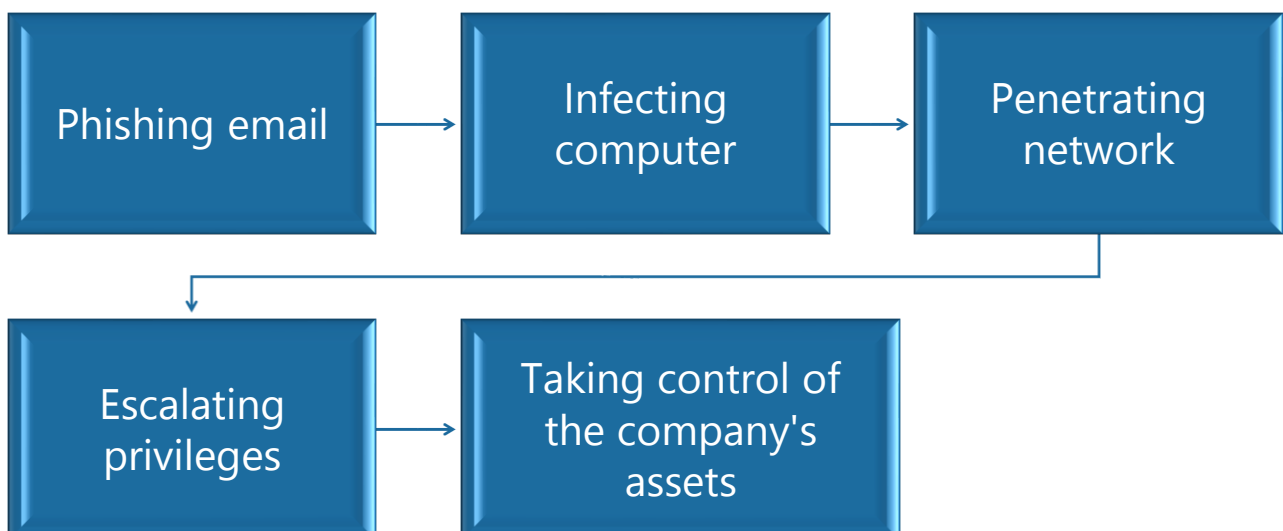
Cybercriminals always follow the money and flexibly react to any changes in the business community. COVID-19 forced an unprecedented number of companies around the world to allow their employees to work remotely. Because the companies had to do it all of a sudden, they were not ready to provide the appropriate security level of this process. And as the vast majority of staff members in most companies were not aware of cybersecurity issues and techniques, they became the easy-to-hit marks for cybercriminals right off the bat.

The employees started connecting to their companies' networks from their own laptops and desktops that in many cases even didn't have an antivirus installed. For attackers worldwide, this situation opened up an unprecedented chance to successfully penetrate networks all over the world.

The process of such an attack is not much complicated. Attackers send out a bunch of phishing or spear-phishing emails with a malicious payload, usually disguised as legitimate Word or .pdf document. When a victim runs the file, her computer gets infected (often with a shell-based backdoor). Thus, the attackers take control of the victim's computer and turn it into a gateway to the company network.



The attack pattern



Cybercriminals on cloud nine

Not only network security was affected by COVID-engendered changes. More and more companies worldwide move their business facilities to clouds, and it makes the cloud environment just another tidbit for attackers.

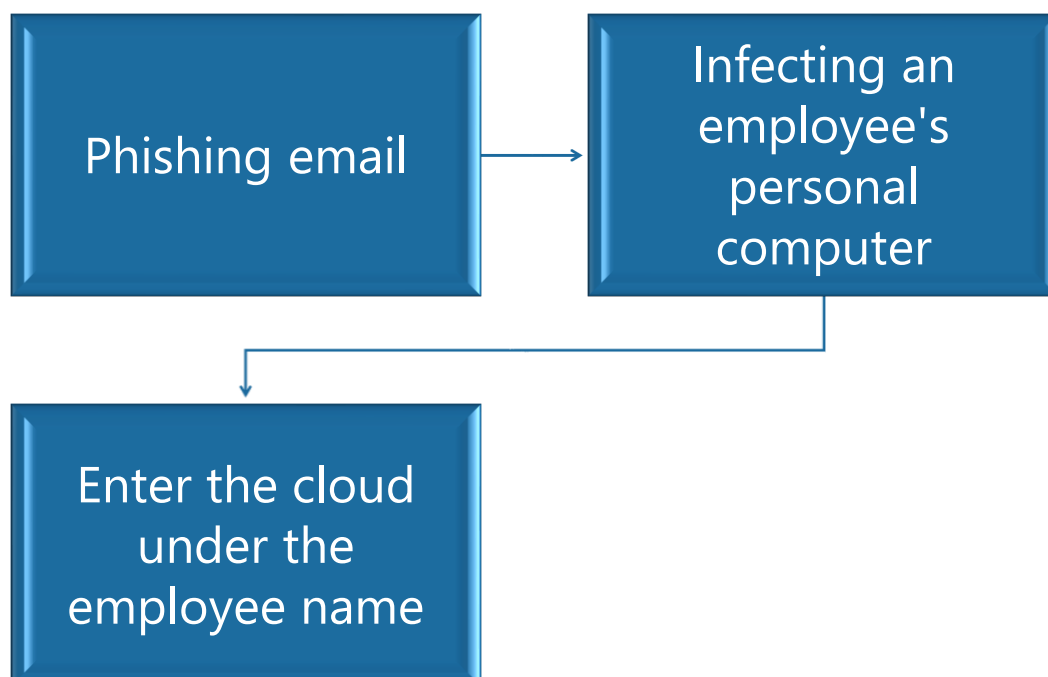
Lockdown made millions of employees connect to companies' cloud facilities every day. Therefore, infecting their computers made the coast clear to cybercriminals assaults.

What makes the situation even more dangerous, in these kinds of attack cybercriminals penetrate a company's

cloud facilities under the name of a real employee, using her credentials and from her IP address, so the security team gets no alerts and stays unaware about compromising... until it is too late.

Because of this fact, we can only guess how many networks were already penetrated by perpetrators covertly and how many attacks remain undetected.

Thus, we can observe a quickly growing vector of cyberattacks in Q3: Attacking employees' personal devices and home computers to get access to company resources.



As a logical follow-up of this process, we observed a huge spike in phishing emails.

Phishing e-mails

COVID-19 provided cybercriminals with a huge possibility for a successful phishing attack they have never had before.

Uncertainty, fear, lack of information and panic are the best friends of social engineers, and living in Q3 2020 was overwhelming with these emotions.

When people experience emotional arousal, they are not able to think critically. Cybercriminals are totally aware of this fact and exploit this human vulnerability to the fullest.

As a result, waves of phishing emails washing over users around the world. These emails targeted companies' endpoints as well as home users. Some of them lured victims into running a malicious file and infecting their computers, others were aimed at stealing credentials. For that last purpose, attackers created clones of the well-

known services' websites that asked to fill out credentials.



COVID 19 FEDERAL GOVERNMENT GRANTS

The Federal Government has ordered weekly the payment of #8500
to all citizen above the age of 18 years

To receive your share of the grant, fill the form below with your correct details.
and then go to the next step.

Provide your Full Name

Provide Residential address

Phone Number

Email Address

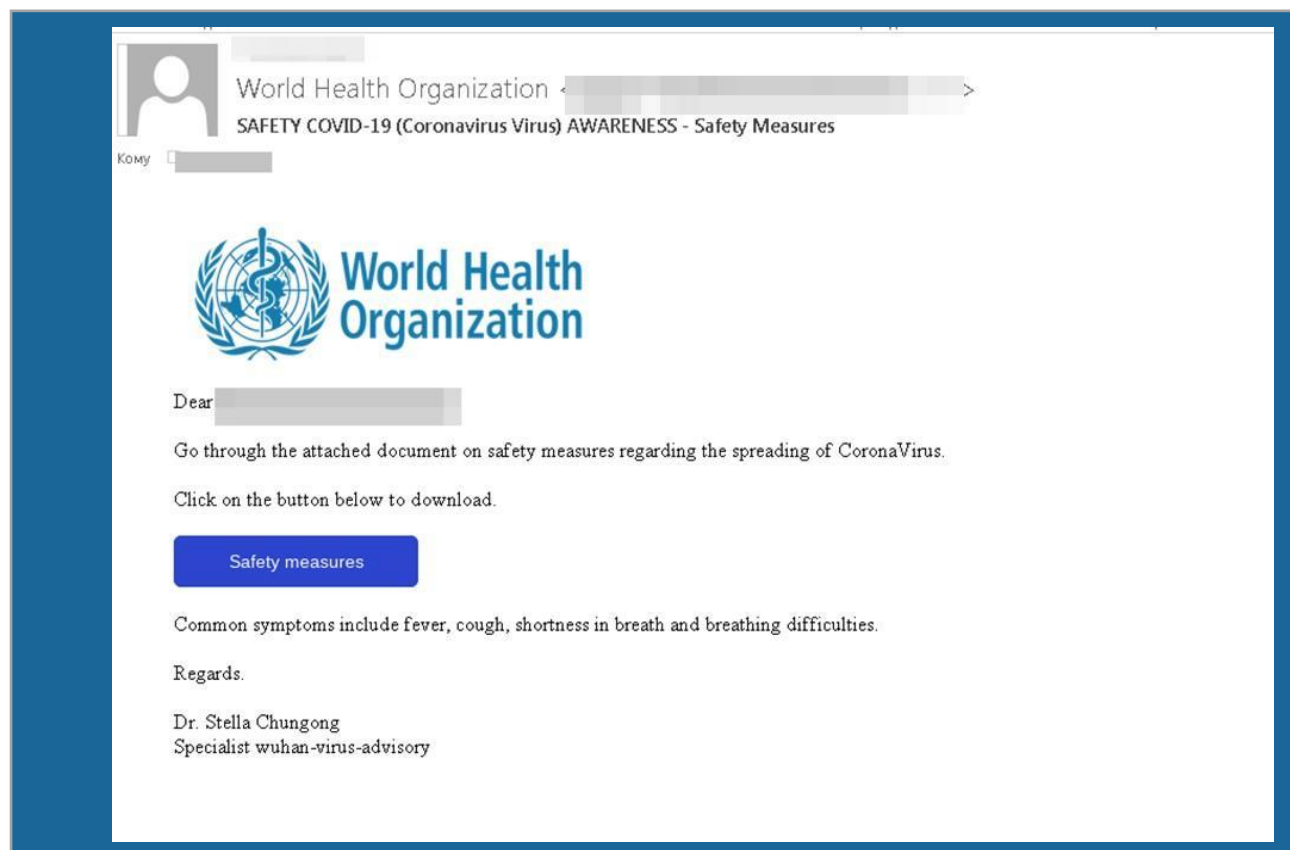
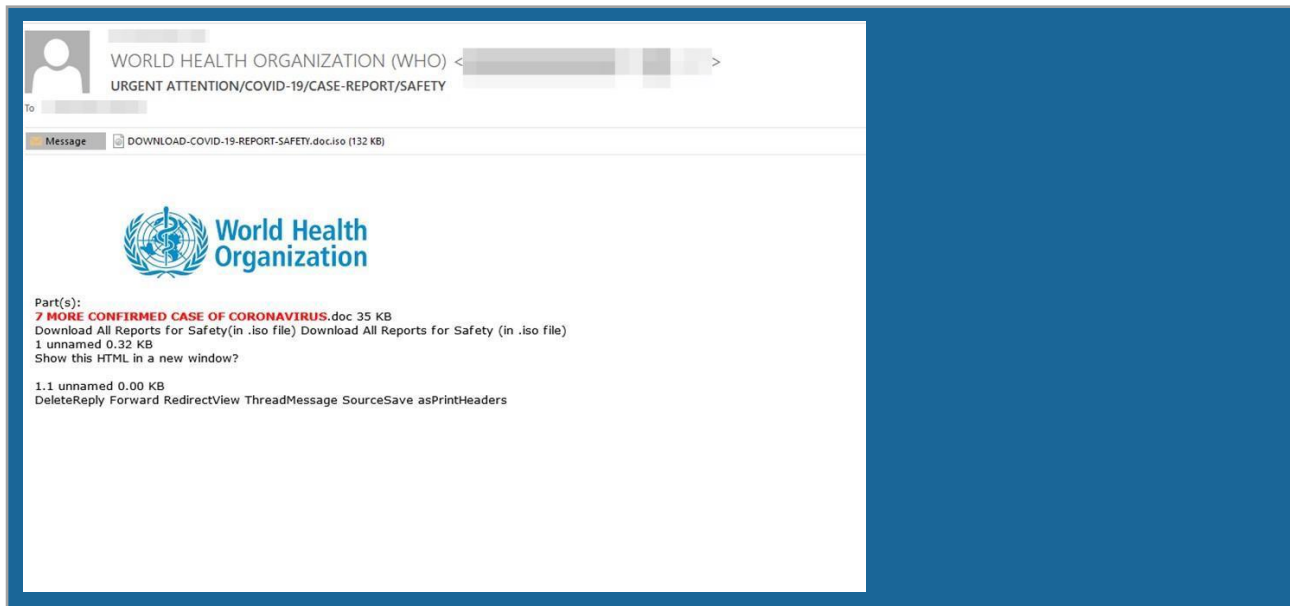
SELECT YOUR BANK

Step 2

Ransomware under COVID-19 influence

As you know, ransomware is a kind of malware that encrypts files on a victim's computer to extort a ransom for decrypting the files. Ransomware dissemination in Q3 was closely linked with COVID-19 phishing attacks. Adding ransomware to a phishing e-mail disguised as a COVID-related document highly raised the chances the attack would be successful: Starving for information that could save their lives, people hooked the bait and run the malware much more often.

Besides ransomware, the attackers added to phishing emails other malware, mostly backdoors and trojans like Fareit that steals login credentials and sends them to the cybercriminals' C&C servers.



Mobile threats: FakeSpy uses fake post-services

The number of mobile device users around the world grows exponentially, and so does the number of malware for these devices. In DIESEC's expert's opinion, the most noticeable Q3 attack in this field is spreading FakeSpy malware targeted for Android devices.

FakeSpy steals private information including the contact list, phone number, device's IMEI, mobile network provider, registered accounts, etc. Then it sends this data to the attackers' Command&Control server. It takes SMS on the infected device under total control (reading, receiving, and sending) and gets access to the information on the external storage.

To top it off, it intercepts every incoming SMS and sends it to the attackers' servers, including the message body,

phone of the sender and time of receiving it. It also checks the infected device for the presence of banking and cryptocurrency applications and looks into the NPki (National Public Key Infrastructure) folder to extract certificates relevant to financial transactions.

FakeSpy is disseminated via the SMS phishing (smishing) attacks. A victim receives an SMS that informs her that the local postal service tried to deliver a package but did not catch her at home, and she will find the details by the added link. Hooked with curiosity, the victim clicks the link and gets to the postal service website with a prompt to install the postal service application. As you probably guess, the website is phishing and the application, in reality, is a FakeSpy malware.

Even after taking total control over the infected device, FakeSpy does not stop. It continues propagating itself by automatically sending the malicious SMS to all contacts of the victim, thus turning the infection process into a never-ending story. But what is really impressive here is the scale and scope of the attack. The malware has a wide range of different guises to imitate postal services according to the country where the victim lives. There are versions camouflaged as United States Postal Service, Royal Mail, Deutsche Post, La Poste, Japan Post, Yamato Transport, Chunghwa Post, Swiss Post...



These postal companies are well-known and widely used by clients. No wonder, many people around the world fell prey to this scam, as they found the SMS plausible and decided to install the "postal" application, with all sad consequences. As we can see, the social engineering element in this attack is crucial.

The trend estimation

Putting it together, we want to highlight the meaningful and interesting fact: The obvious growth of using social engineering techniques.

Each of the aforementioned attacks, be it stealing credentials, taking control over an endpoint, penetrating network or cloud, implanting backdoor or infecting with ransomware, includes a power element of Social Engineering or Human Hacking. In the first turn, the attackers targeted human minds by using various psychological tricks.

We believe that this trend will continue growing in the near future and the role

of Social Engineering will become even more considerable. There is a solid reason for that: People remain the weakest link of the security chain. Many companies have up-to-date firewalls deployed and tuned up as well as web-applications hardened, but their employees still are easy targets for an attacker. Contrarily, cybercriminals invent new Social Engineering techniques at a staggering pace.

And this incongruence between the perpetrators' social engineering inventiveness and companies' insecurity creates a huge gap that clearly explains

why so many attacks in Q3 were successful for cybercriminals.

Unfortunately, we suppose that this gap will be growing in the near future, so

many companies who won't take appropriate measures timely and correct their cybersecurity approach will fall prey to these attacks.

You will find out how to harden your protection from Social Engineering in the last part of this review.

Section 2. From DIESEC's Experience.

How to Make Your Cloud Hacker-proof

IT go clouding at a speed of lightning. This process is unstoppable and it's not surprising: Multiple benefits for business are undisputed and obvious. But with progress and profit come new dangers. Alongside with the benefits, this process brings new, complicated, hard-to-solve challenges in the security field. Cloud security requires special, immaculate approaches.

Nowadays, when most parts of assets are digital, a company's cloud protection is often a question of the entire business's survival. Meantime, the number of specialists qualified enough to build a secure cloud infrastructure is very limited.

As a result, a terrifying number of companies' clouds today are hacker-friendly, which means the companies' assets can be stolen or destroyed at any moment.

DIESEC's experts have conducted testing, securing and auditing of many cloud environments, so here we'd like to share our experience to help other companies to avoid fatal mistakes and pitfalls on this troublesome way.

In this issue, we'll tell about one of the most convoluted tasks that may be required in the cloud environment – elaborating a Digital Forensic Strategy for a world-known financial institution and migrating its digital forensics lab into the cloud.

We call this task one of the most convoluted for several reasons. Firstly, securing a cloud is a hard nut to crack by itself. Secondly, digital forensics is probably the most demanding entity in IT security. Dealing with it, you need to take into attention a lot of factors – failing even with one of them can come to devastating consequences.

We'll talk about these challenges in detail. But let's start with the general nuances of cloud security.

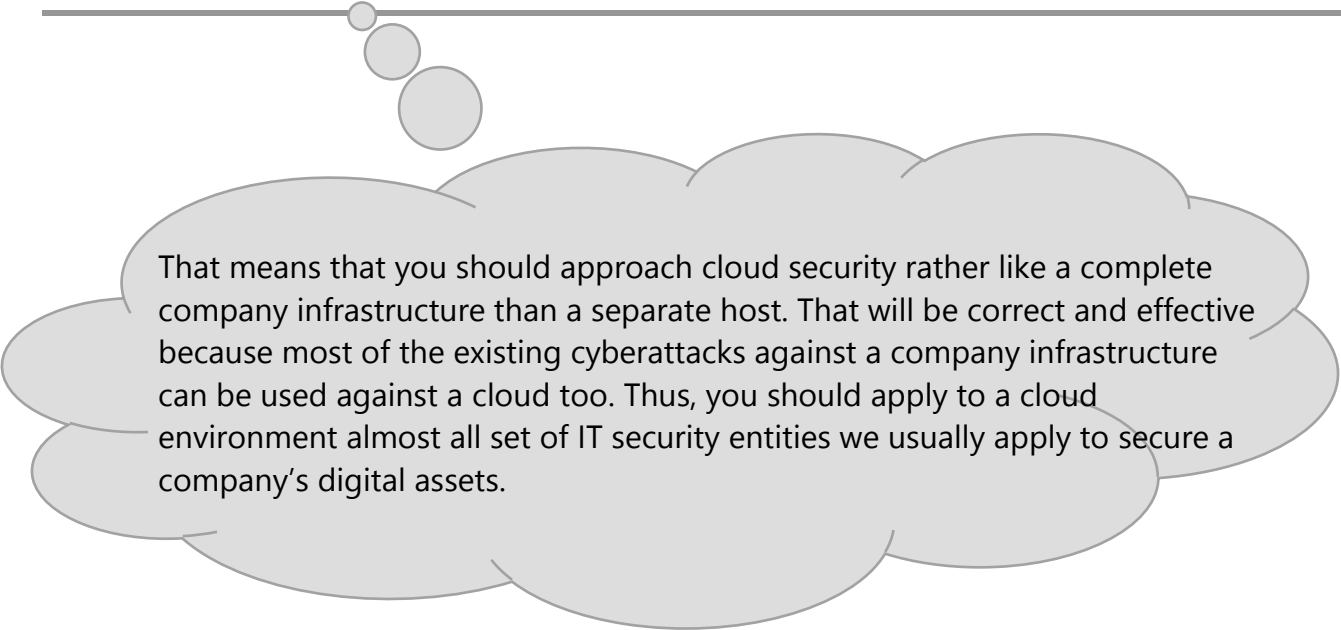
What you need to protect in the cloud

For a better understanding of the security challenges, let's remind what a cloud is in the world of computing. Unfortunately, many people perceive a cloud as "just one more host/server to connect remotely", and this attitude defines their approach to its security. If it's just another host, you can secure it in the same way as others, right?

No, it is totally wrong, and such an approach can cost you millions in losses. Unfortunately, thousands of companies fall prey to this dangerous misunderstanding.

In reality, you cannot consider a cloud as a regular server. It is not just data storage for users to connect, otherwise, there wouldn't be a need in a new name for that. Every cloud has one of the following functions: It delivers services (SaaS) and provides platforms (PaaS) or infrastructure (IaaS). Unlike a regular server, it includes virtualization, separating of space, deploying various web-applications, assigning resources for multiple customers, etc.






That means that you should approach cloud security rather like a complete company infrastructure than a separate host. That will be correct and effective because most of the existing cyberattacks against a company infrastructure can be used against a cloud too. Thus, you should apply to a cloud environment almost all set of IT security entities we usually apply to secure a company's digital assets.

But that's not all. There are additional challenges.

Firstly, there are some special attacks aimed at cloud environments like Session Riding or Side Channel attacks. Secondly, many people use the cloud environment simultaneously and access it remotely, from anywhere.

These factors demand additional attention to optimal implementation of

encryption, authorization, authentication and access control. And don't forget to add the necessity to provide constant availability of the cloud...



To make the long story short, you need to apply near the same package of security measures that you use for your infrastructure and add something more according to the clouds' specificity.

From Firewalls to Humans



To be more precise, cloud security design and architecture must include various security instruments. Technical tools like firewalls, IDS, WAFs, etc. Administrative controls, policies, procedures and so on. Such vital elements of IT security as Governance, Risk management and Compliance should be inevitably applied to the cloud security to be sure that all policies and procedures are correctly implemented and

followed, risks are assessed and mitigated and legal requirements are not violated.

But the first step you need to do is building a cloud security strategy.

The precise strategy depends on the exact specificity of the cloud you are going to protect. You should consider many factors to elaborate on it correctly.

For instance, are you going to use the cloud as IaaS (Infrastructure as a Service), SaaS (Software as a Service) or PaaS (Platform as a Service)? Strategies for each of them will differ from each other in some elements.

Do you want your cloud to be public or private? If it is public, you can't control the whole security vectors. Part of them inevitably will be under control of your cloud provider. You have to decide if it's suitable for your situation or you'd better choose a private cloud that will be totally in your hands.

Maybe, a hybrid cloud that includes parts of both public and private cloud will be the best solution?

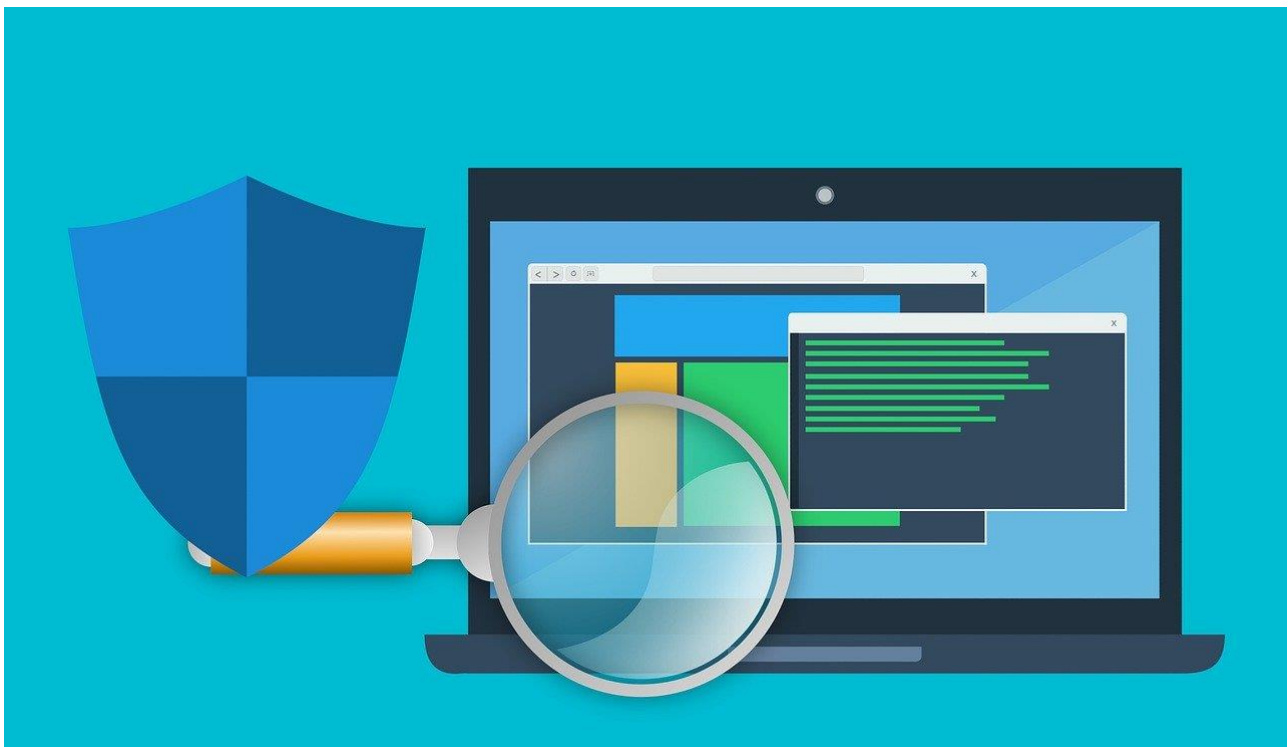
As you see, there are plenty of questions to answer before implementing the cloud security strategy. But they increase significantly when it comes to cloud digital forensics.

The Secrets of Digital Forensics Implementation

While cloud security itself is a complicated multilayer mechanism, digital forensics requires a much more sophisticated mastery approach. And here is why.

Let's start from the main point of digital forensic: all data should stay unchanged, otherwise, it can't be accepted for a court case as evidence. In case the procedures of gathering, storing or transferring this data were violated, their worth goes down to zero.

Recently, digital forensic specialists used to analyze hard drive images or memory dumps on a single machine separated from the Internet. Of course, doing such work in the cloud brings a lot of sound benefits in speed, resources and various software. But...



There are strictest standards for handling digital evidence. It's rather hard to follow all of them even if you work on a devoted computer, but when you go cloud, the situation is a

thousand times more complicated. Now the data is not on your isolated machine only. It travels through the network back and forth and is stored

and processed in the cloud – a remote host that plenty of people have access.

That brings us new threats and challenges. Let's have a close look at them.

As you remember, our primary goal is to guarantee the integrity of the data - otherwise, all digital forensics work will be mistrusted and senseless.

Different threat actors want and can destroy data integrity. In the first place are cybercriminals interested in terminating or stealing those data in any possible way to avoid being tracked down and arrested.

And it's not just about the cybercriminals whose crimes are investigating by the digital forensic lab specialists at the moment.

Any digital forensic lab is a threat to cybercriminals in general because it discovers their methods and malware for committing cybercrimes. Thus, any digital forensic lab is an attractive target for perpetrators and must always be considered as an object of high-degree risk in the firing line.

Also, you should not forget about not-too-moral competitors who may want

to get access to the secrets of your company.

Thus, we have plenty of serious threat actors longing to unleash a diversity of attacks on the lab. Besides that, the data can be damaged accidentally because of the negligence or incompetence of an employee or a tech glitch as a result of incorrect software implementation.

And don't forget that a digital investigator does not work with an original image but uses copies of them. So you need to provide both storing the images and transferring their copies via the network in a 100% secure and reliable way.

Thus, the task is not only to make the cloud bulletproof to any attack but also to guarantee that data can't be leaked, changed or destroyed during the transit or affected by an insider



Add general rules and methods of cloud security to these digital forensics demands – and you'll see the basic set of challenges for building a digital forensic lab.

Some Security Tips to Remember

For obvious reasons, we can't publicly share the details of how exactly we overcome those challenges building a digital forensic lab for our client. The good news is there is no real need in it because every task of such kind demands its own approach, strategy and implementation depending on the

company's individual objectives and specificities. But what we definitely can share is the list of the points that need primary attention when you do a job like this.

Here are the main factors to take into consideration.



As a cloud can be vulnerable to the most known kinds of cyberattacks, you should apply to it the most of the security standards and tools you apply to the company's digital infrastructure.



To guarantee data integrity, take care of the reliable encryption of Data- in-Rest as well as the Data –in-Transit. Give special attention to the encryption key storage.



Give special attention to implement proper access controls based on the least privilege concept. Carefully elaborate authentication and authorization procedures and processes to make impossible stealing credentials or getting an unauthorized access. No doubt, multi-factor authentication is a must.



All activities of all users should be monitored and logged carefully, so it would be definitely clear who did what and when. Of course, the monitoring system must be properly implemented to protect the logs from deleting or modification.

How to implement cloud security in the best way

Today there are various tools and software, open-source and proprietary, to build, test and secure cloud environments, and you have to choose those ideally suitable for your tasks.

This is why the main success factors here are the correctly elaborated strategy and its high-professional implementation. The strategy must define not only what the software to use but how to combine it in one effective mechanism that doesn't have conflicting parts. More of that, this mechanism should work quickly and reliably.

"Infrastructure as a Script" is a good approach to meet this goal. Basing on this approach, our specialists combine all cloud tools with customized scripts for better and smooth performance, and it inevitably brings excellent results.

And last but not least idea to take away. Even if you are not going to build a Digital Forensic lab, these recommendations will be useful for you. Why? Because they are applicable to any cloud environment that requires the top-standards, enhanced security.

Section 3. The Attack of the Quarter.

How to Avoid Being Hacked Like Twitter

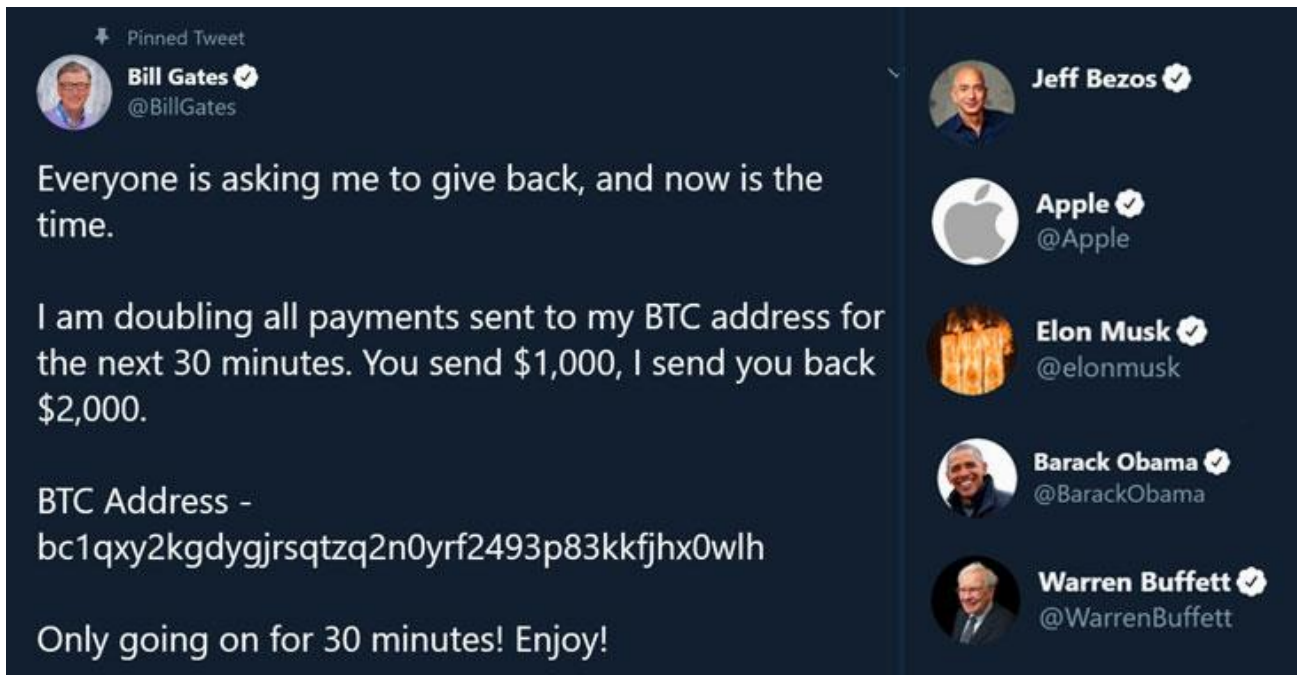
The recent Twitter hack quickly became one of the top news in the world. And there are at least two solid reasons for this. Firstly, the security system of such a powerful company as Twitter occurred to be flawed. Secondly, the attackers were able to break into accounts of the most powerful people of the world with frightening ease. Inevitably, the question arises: if such a powerful entity can be hacked with such ease, might we believe that average companies and people are really secure today?

That is why it is especially important for the cybersecurity community to deeply elaborate on this attack and learn lessons for the future to prevent assaults of this kind. Here is the DIESEC analysis of the situation and our recommendations on your protection.

The attack: Would you like to double your money?

On a one splendid July day, followers of Bill Gates discovered an unusual tweet, promising them to double any sum sent to the given bitcoin address. They were not alone. The same text appeared in the accounts of many

celebrities, top businessmen, blue-chip companies and politicians, including Elon Musk, Barack Obama, Jeff Bezos, Mike Bloomberg, Joe Biden, Apple, Warren Buffet, etc.



Of course, the owners of those accounts did not write those tweets. The accounts were hacked. And it is, probably, the most stunning and massive attack on powers-that-be and celebrities for the moment.

"We're embarrassed, we're disappointed, and more than anything, we're sorry. We know that we must work to regain your trust, and we will

support all efforts to bring the perpetrators to justice," Twitter wrote in their blog.

And they really have solid reasons for "disappointment". Many observers are wondering: What the consequences would be if the attackers were not just scammers looking for some cash but terrorists or psychopaths wanting to wreak havoc and panic?

The attackers: Exploiting human vulnerabilities

Soon FBI busted the supposed attackers. The feds have accused three young men: 17-year-old Graham Clark, 19-year-old Mason Sheppard, and 22-year-old Nima Fazeli. And here is the spot where interesting nuances appear.

According to the FBI, some of the detained were accused of fraudulent

actions before. But they don't look like technically advanced super-hackers. And it's a very important point to take into consideration. This staggering attack was not based on sophisticated techniques of computer hacking but social engineering tricks. In other words, it was not hacking computers -- it was hacking of human minds.



Why do we want to stress this point? Because it clearly reflects the current situation in the cybersecurity field: Most attacks are targeted at humans, and today there are not enough tools

to protect from attacks of such kind. At least, much less than from tech-based assaults.

We suppose the Twitter network environment and web-applications have the best defensive equipment possible. But as you can see, it goes useless when it comes to human vulnerabilities.

The most impressive thing about this attack is that some people with fraudster skills could easily break into one of the most powerful tech companies in the world. And what is more impressive, their tricks were not so sophisticated. They broke into Twitter in just two steps. Let's look at them closely.

The method: from Slack to spear-phishing

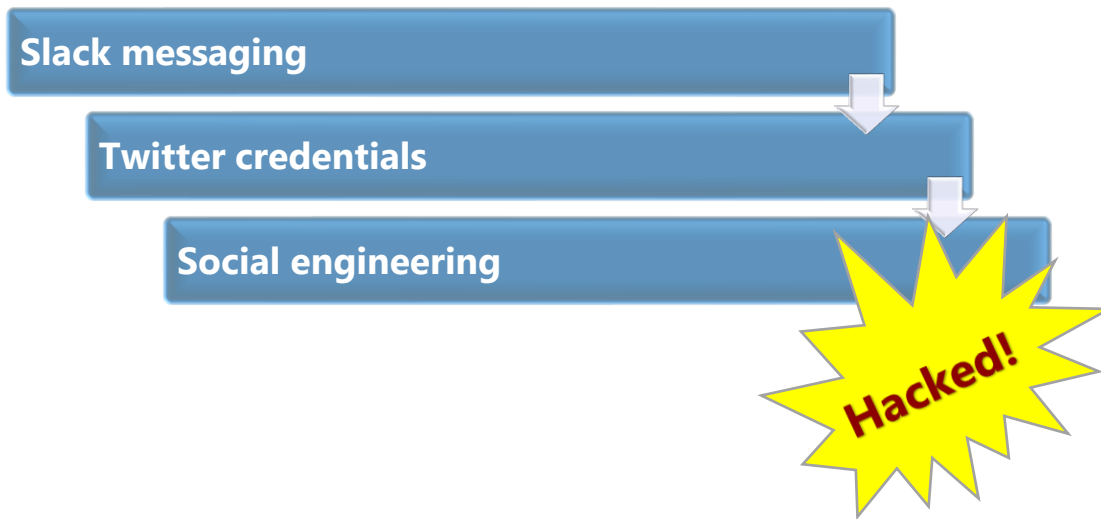
As Twitter disclosed the attack details rather reluctantly and sparingly, we based our research on the most influent media reports.

As NYT reported, one of the attackers "... got access to the Twitter credentials when he found a way into Twitter's internal Slack messaging channel and saw them posted there, along with a service that gave him access to the company's servers".

That is an epic fail number one. If you save credentials in this way, being hacked is just a matter of time.

But wait... just credentials must not be enough to enter the Twitter internal network. It must have a two-factor (2FA) authentication, right?

Right. And that's why the perpetrators made use of social engineering. They conducted a spear phishing phone attack to get the information from Twitter's employees. What is especially interesting, they used the as-old-as-time trick: as Reuter reported, the caller pretended to be a co-worker from the IT department and convinced the employee to share credentials.



Can we call it a refined and sophisticated attack? Unlikely. In fact, “easy-peasy” sounds much more applicable.

Let’s sum up now. Three young men, one of which underage, without applying deep technical knowledge,

hacked one of the most powerful tech companies and took control over accounts of the most powerful people on the Earth.

Don’t you think there is something wrong with the approach to cybersecurity, do you?

Lessons to learn: Strengthen the human factor

A few obvious questions inevitably arise here. What mistakes and flaws in Twitter’s defense line made the attack successful? How can they be corrected in the future? Was it possible to prevent the attack?

Based on the information above, we can make a clear conclusion: the attackers succeeded because Twitter’s security approach and implementation were not corresponding to top-security standards. Here is why.

Firstly, it’s obvious that their security policies and procedures were not implemented or at least followed correctly. Storing credentials into a Slack account is a definitely rude violation of general security rules.

The other security drawback is giving access to a wide range of people. As Reuter reported, “More than a thousand of Twitter employees and contractors as of earlier this year had access to internal tools that could

change user account settings and hand control to others, two former employees said”.

Here we can see the rude violation of Access Control rules. The correct approach supposes limiting access to only the necessary number of employees.

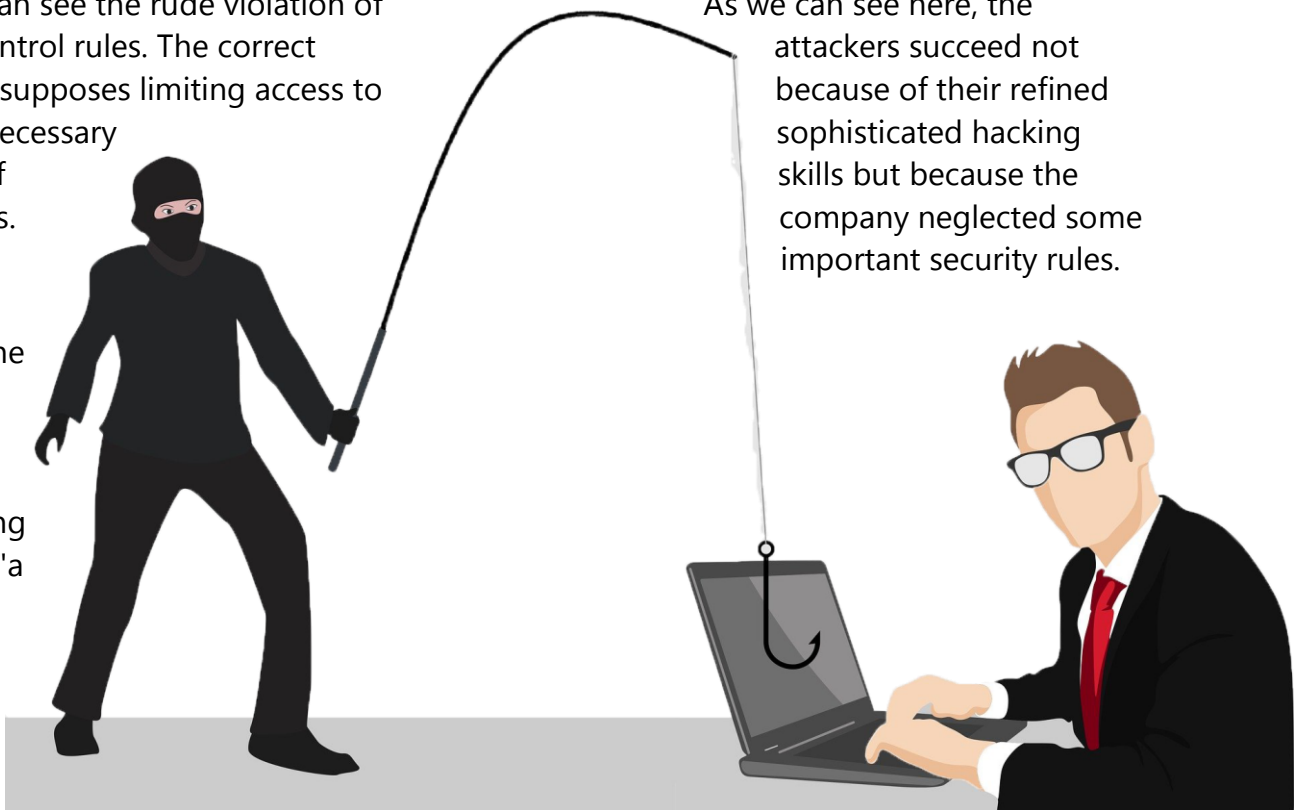
And the icing on the cake. The social

engineering trick with "a colleague from IT-

department" is so old and trivial that is considered a classic example of SE and explained on any decent security

training. Frankly, it looks rather strange for employees of such a solid company to buy into that.

As we can see here, the attackers succeed not because of their refined sophisticated hacking skills but because the company neglected some important security rules.



What is important to notice, those rules don't relate to networks and web-applications but a human factor.

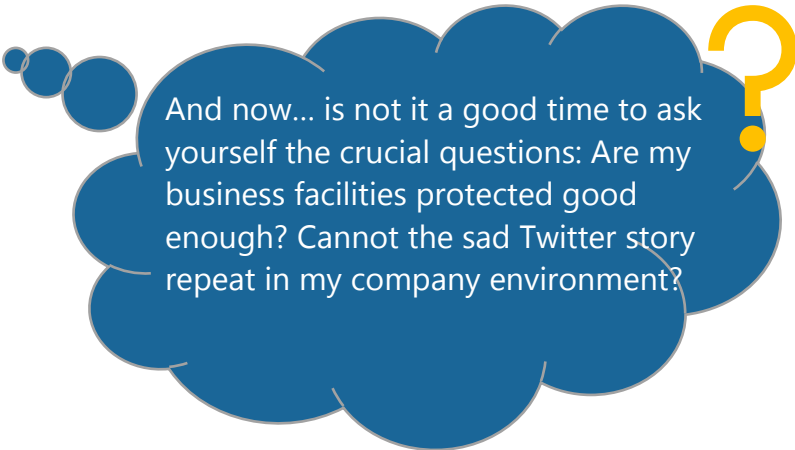
How you can avoid falling prey like Twitter

Firstly, you should elaborate and implement strict policies and procedures about passwords, including its storing and secure handling.

Secondly, you need to apply strict Access Control rules, particularly the principle of least privilege that allows a user to work only with functions necessary for his/her duties.

Thirdly, conduct a decent training of employees on counter social engineering skills. As a result, your employees must be able to spot most kinds of social engineering attacks and take correct action to stop or mitigate the attack immediately. That is how we in the DIESEC train staff of our clients.

Yes, just these three simple steps taken promptly could save Twitter from the shame and troubles they have today.

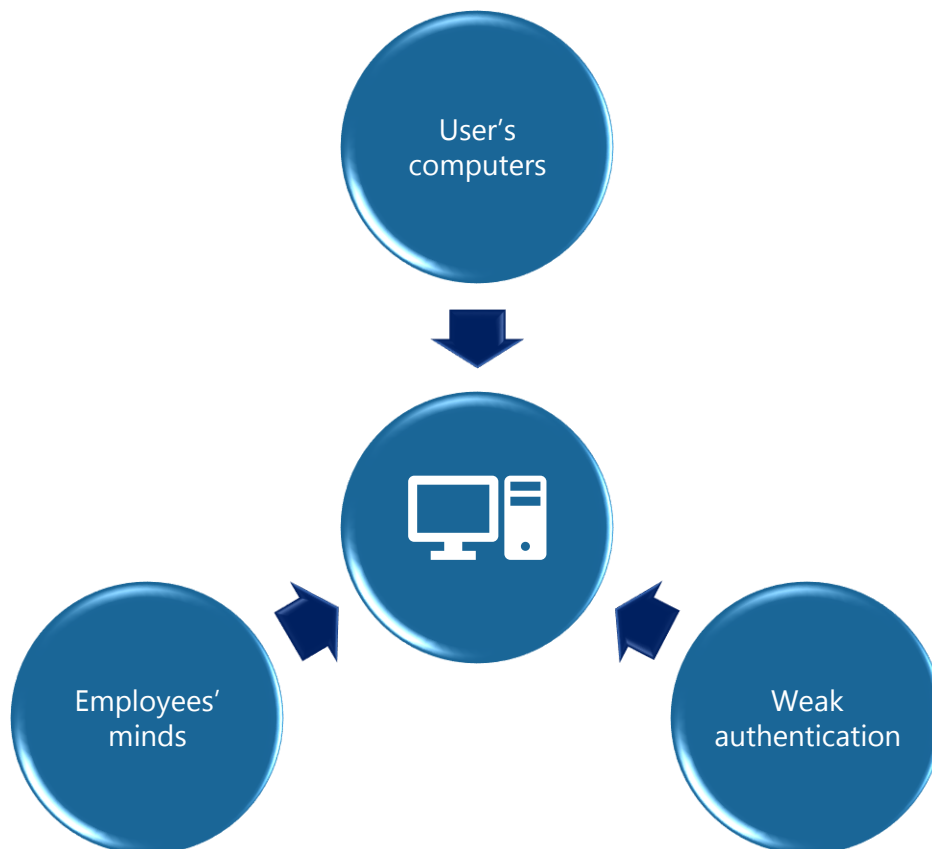


And now... is not it a good time to ask yourself the crucial questions: Are my business facilities protected good enough? Cannot the sad Twitter story repeat in my company environment?

Section 4. Protect Your Assets. **Going In-depth**

What is the best way to protect yourself from the COVID-inspired cunning attacks that cybercriminals unleashed in the last quarter? For this purpose, we propose a two-step strategy. Firstly, we need to define the most vulnerable spots that make companies easy targets for perpetrators. Then we need to understand how to mitigate or block these weaknesses.

Vulnerable points



1. **Users' personal computers.** Many employees have started working from home with their own devices, and the vast majority of them are not aware of cybersecurity problems and the necessity to take precautionary measures. Nor they are aware of different kinds of ways perpetrators can attack them, neither have they security software on their computers installed and tuned up properly.
2. **Weak authentication and authorization** of a company digital facilities (network, clouds, websites). Imagine a situation when attackers penetrate an employee's computer. In many cases, users store their passwords in clear text in a file on the desktop. Or, what even worse, they can keep them in messengers like in the sad story of the Twitter hack. All the attackers need to do is to take those credentials and enter the company's network or cloud facilities.

But even if employees do not keep their credentials so recklessly, the perpetrators are still can easily penetrate the company facilities. All they need to do is to extract the cookies from the victim's browser, and voila – they are inside the company.

3. **Employees' minds** are vulnerable to social engineering attacks. As you may notice, social engineering techniques became a real hit among cyber attackers in Q3 2020. The most dangerous thing about it is that an average person cannot resist to the refined manipulative techniques of perpetrators. The attackers constantly train and hone up their social engineering skills and invent more and more cunning tricks to hack humans' minds. As a result, almost any employee can fall prey to such attacks. As a not-so-old proverb said, "There is no firewall for a human mind".

The ABC of Defense

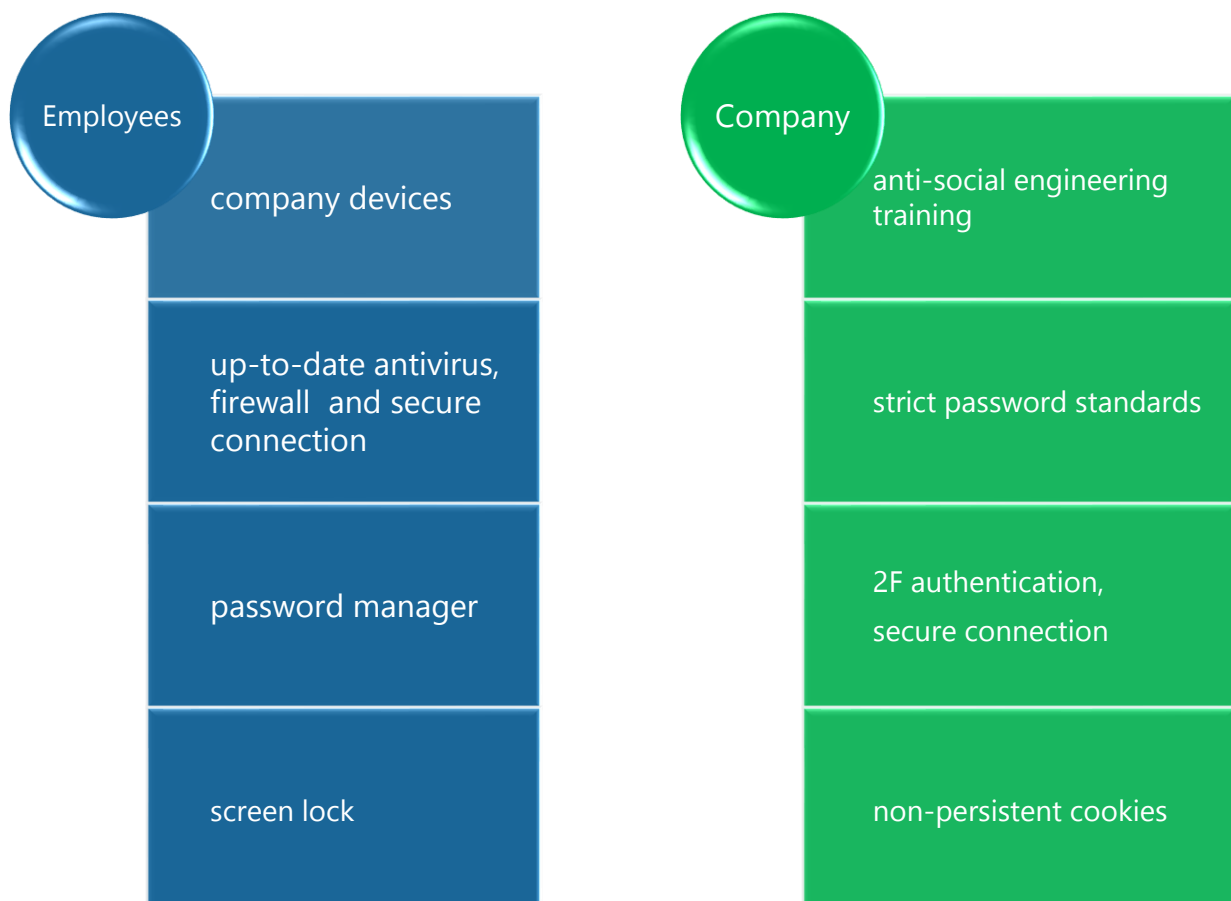
What you need to take into attention to build a reliable defense line is understanding the fact that scattered steps will not be effective. You need to build a system based on the defense-in-depth principle that consists of mutually supportive elements. This system must include a combination of policies, technical tools and staff training.

1. **Policies.** You need to elaborate on strong work-from-home policies. These policies must combine using technical tools of defense with rules of behavior. The best way to high-level security is to provide your employees with the company devices (with pre-installed security software) that must be used for working purposes only. Of course, if a company cannot afford it, using an employee-owned device is another option. In this case, some rules must be followed including mandatory use of up-to-date antivirus, firewall, and following the rules of secure connection.

2. **Authentication** security needs hardening on both sides. On the company side, it must be implementation of secure connection and strict password standards. Besides that, we recommend using two-factor authentication wherever it is possible. In this case, even if attackers steal a victim's credentials, they still have to bypass 2F authentication, so the company assets remain secure. To avoid session hijacking you should use non-persistent cookies (valid only for one session).

On the employee side, the policy should restrict keeping passwords on a computer in any other way than in a reliable password manager or an encrypted file. Every employee should always use a passworded screen lock for their computers to avoid the access of unauthorized persons.

3. The risks of **social engineering attacks** can be mitigated by staff education. Mandatory training for employees on social engineering, especially phishing, can neutralize up to 87% of attacks if conducted correctly. As a result of the training, an employee must know the most popular signs of such attacks to recognize them, ignore cybercriminals requests and report to the security department.



Section 5. What is Coming Up?

COVID -19 amply demonstrated how “black swans” in the physical world radically influence the situation in the cyberspace in general and the cybersecurity field in particular. We suppose this trend will continue in Q4 2020 and even far beyond it in 2021. Thus, to predict the upcoming situation in the cybersecurity field we need to have a look at the main expected events of the physical world. For this purpose, we would highlight the following trends.

As the second wave of COVID-19 is supposed to strike the world in Q4, its course of events will determine many aspects of the cybersecurity trends. The harder is the impact of the second wave, the sharper spike of cybercrimes we will observe. There are a few reasons for that.

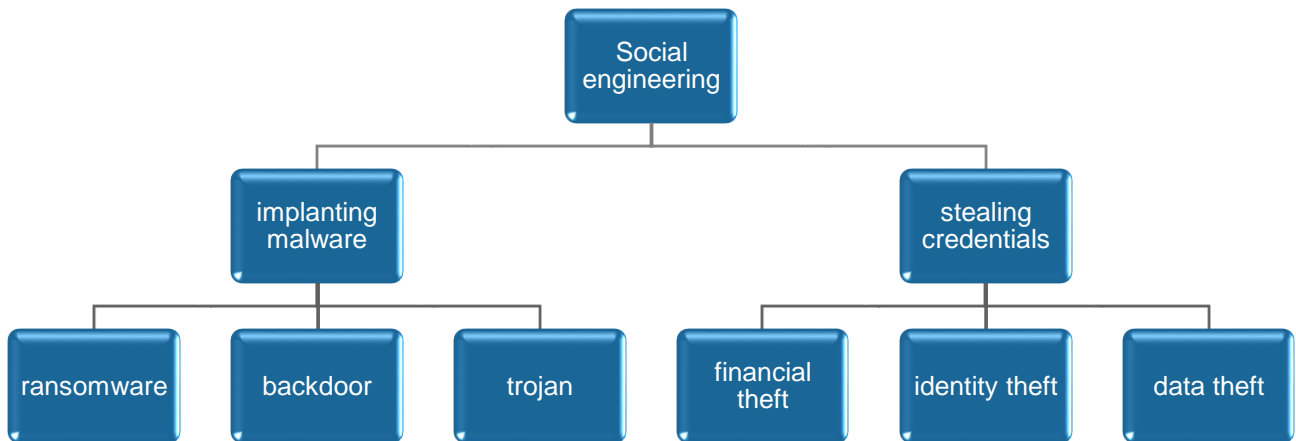
Firstly, prolonged lockdown will result in significant growth of the work-from-home trend that will entail the growth of all the aforementioned risks and the number of companies under threat.

Secondly, the next COVID-19 wave will engender a new spike of fear, panic, and anxiety. A person in such an emotional state is not able to take correct decisions, and it makes employees much more vulnerable to social engineering attacks.

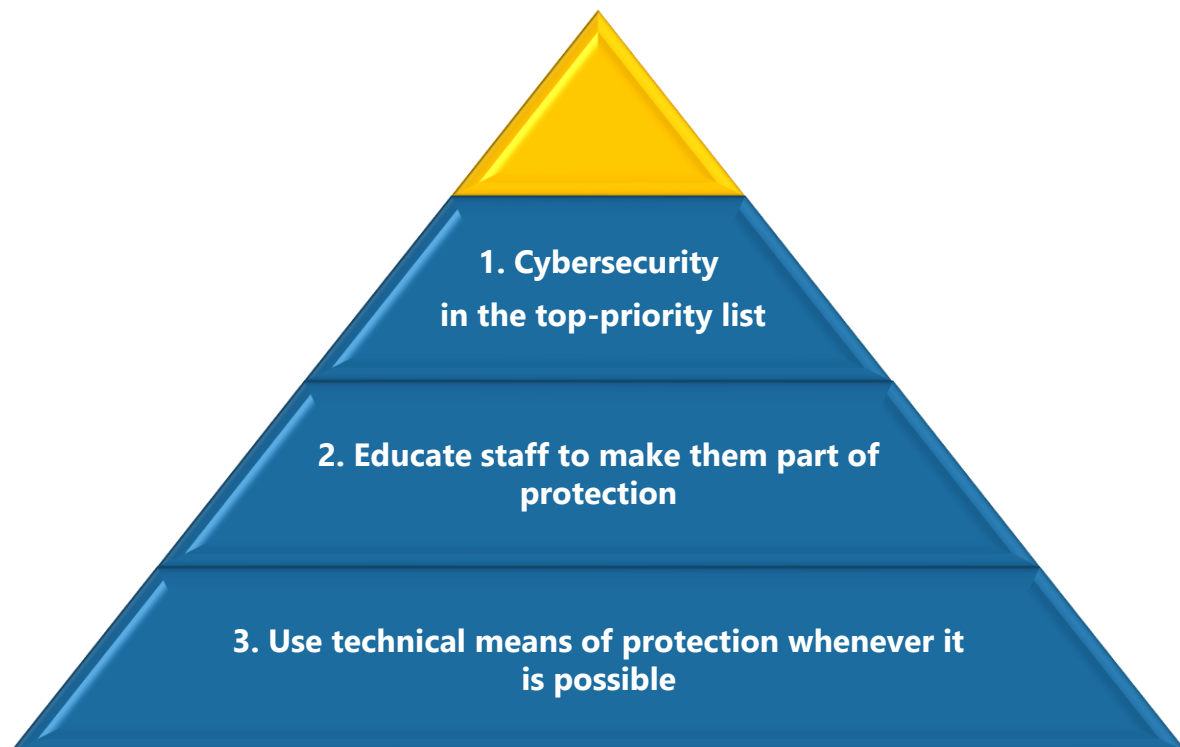
Thirdly, most companies are going through the transitional period from “work-in-the office” to “work-from-home” or “work-from-home combine

with work-in-the office” models. In such a period of radical changes, a company is extremely vulnerable: the regular security techniques cannot be effectively applied to the new reality, while up-to-date techniques and methods are not elaborated and implemented yet. To top it off, most companies in the first turn care about organizing the work-from-home process, putting off security measures as subservient.

Putting it together, we conclude that COVID-19 will continue to be an influential factor determining the situation in the cybersecurity field. It means that, with a high likelihood, we will observe growth in the number and sophistication of social engineering attacks as well as the appearance of new modifications of backdoors, trojans and ransomware. In the opinion of the DIESEC's experts, the scheme of the most popular attacks in Q4 will look as follows:



To withstand this upcoming threat effectively, we recommend the following “pyramid” of three basic principles:



1. Get your priorities straight. In uncertain times risks grow exponentially, so the cybersecurity measures must be on the top in the to-do- list of your company.

2. Educate your staff about the cybersecurity problem. This approach relates to the defense-in-breadth security principle: The more employees are cyber security-aware, the easier it is to protect the company's assets.
3. Meanwhile, take into attention the unstable emotional state of people during the pandemic. It means you should give priority technical means over human ones. The best practice in the current situation is to use technical means of protection whenever it is possible.

We hope that by combining these principles with other knowledge outlined in our Review, you will successfully get around all cybersecurity risks and dangers lurking in the upcoming Q4 2020.

Live informed and secure with DIESEC!

If you have any questions, please feel free to get in touch with us by the contacts below.

Q3

2020

**Mergenthalerallee 77
65760 Eschborn
Germany**

**Phone: +49 6196 202122 0
Fax: +49 6196 202122 99**

**Email: info@diesec.com
Web: <https://diesec.com/>**

**The USA office:
DIESEC INC
20130 Lakeview Center
Plaza
Suite 400
Ashburn, VA 20147
United States**

Phone: +1 703 665 3780