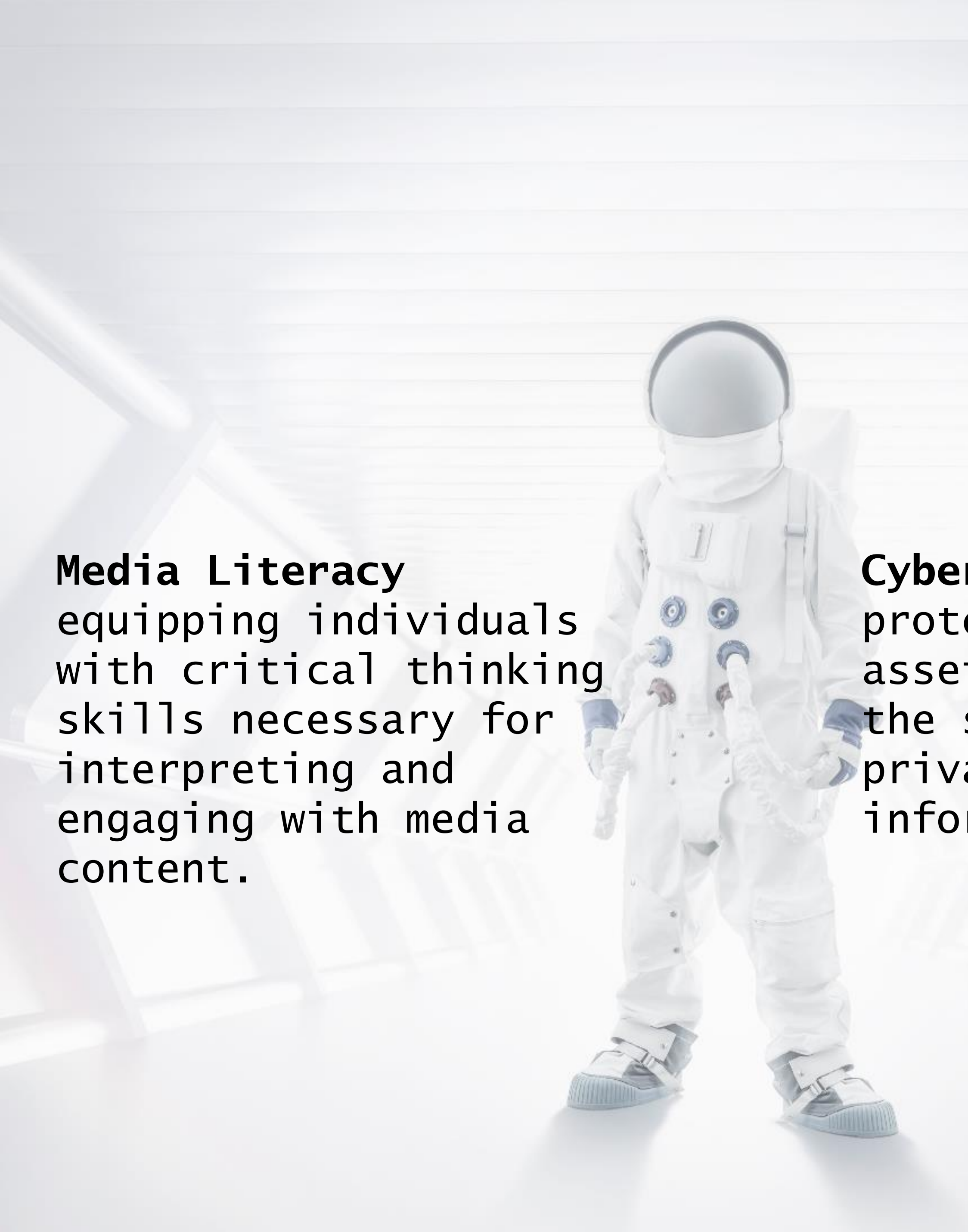
New Trends in Cyber Security

Understanding Risks, Threats, and Incidents, with Focus on Teachers

Aleksandar Acev, CISM, CISA

aacevs@gmail.com



Media Literacy
equipping individuals with critical thinking skills necessary for interpreting and engaging with media content.

Cyber
prot
asse
the s
priva
infor

Objective

WHAT:

- Understanding of cybersecurity risks, threats, and incidents,
- Connection between Cybersecurity and Misinformation (Fake news)
- Discussion and examples on Ideas for activities for increasing resilience to cyber-attacks

HOW:

- Learning through analysis of real-world cyber incidents
- Interactions and Discussion
- The importance of Gamification

RESILIENT TEACHERS, STUDENTS AND SCHOOLS

DISCUSSION POINT: EXPERIENCES WITH CYBER ATTACKS

DISCUSSION AND ALL SESSION INFORMATION IS UNDER CHATHAM HOUSE RULES!

The Chatham House Rule is an agreement between meeting participants that allows people to use the information from a discussion, but they can't say who the speaker was, or what organization they're from. Once the Chatham House Rule is invoked, it's binding to all participants.

- Have you or your schools experienced a cyber attack?
- What happened?
- How did you deal with the attack?
- Were there any lessons learned?
- Did the attack initiate overall increase in interest into cybersecurity, of the priority on cybersecurity in your school?

RISKS, THREATS, ATTACKS AND INCIDENTS

"Cybersecurity is the art and science of protecting digital information and systems from unauthorized access and damage."

CYBERSECURITY RISKS AND THREATS IN THE DIGITAL CLASSROOM

Threats: These are potential malicious actions or events that can cause harm. They represent the **“WHAT"** in terms of potential dangers.

Risks: These are the potential negative outcomes or impacts resulting from threats exploiting vulnerabilities. They represent the **“SO WHAT"** in terms of the potential consequences or impact of the threat.

Threats:

1. Phishing Attacks
2. Ransomware
3. Distributed Denial of Service (DDoS) Attacks
4. Malware (viruses, worms, trojans, spyware)
5. Insider Threats
6. Social Engineering

Risks:

1. Physical Theft or Loss
2. Unpatched Software
3. Internet of Things (IoT) Vulnerabilities

CYBERATTACKS AND INCIDENTS ON SCHOOLS

CASE ANALYSIS

SCHOOLS VS. AIRPORTS

"Any event that threatens the integrity, confidentiality, or availability of digital resources."

CYBERATTACKS ON SCHOOLS

TOP 5 TYPES OF CYBER-ATTACKS ON SCHOOLS

1. **Increase in Ransomware Attacks:** where cybercriminals encrypt critical data and demand payment for its release.
2. **Phishing Attempts**: with attackers targeting students and staff through deceptive emails to steal sensitive information.
3. **Distributed Denial of Service (DDoS) Attacks**: aimed at disrupting online services, especially during exam periods.
4. **Data Breaches**: involving the theft of personal and financial information have affected numerous schools across Europe.
5. **Malware and Spyware Infections**: The use of malicious software to infiltrate and monitor educational networks has been a consistent threat.

https://corporatetraining.usf.edu/blog/top-5-k-12-cybersecurity-threats-schools-are-facing

https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done

CYBERATTACKS ON SCHOOLS

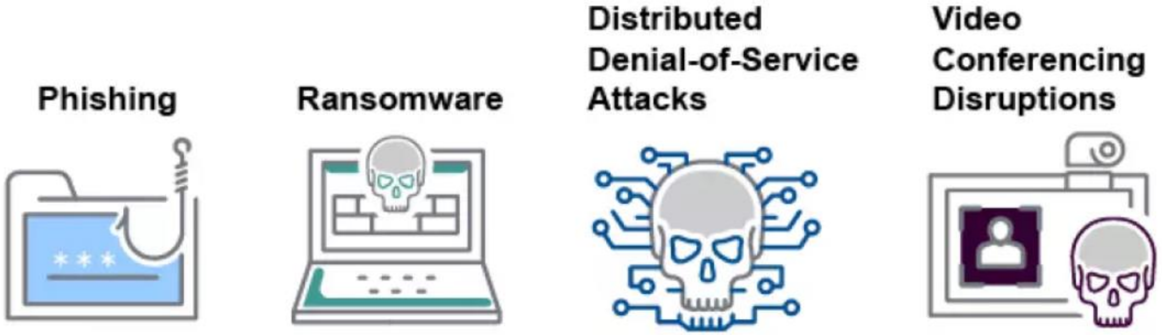
WHAT ABOUT THE REPUBLIC OF NORTH MACEDONIA?

1. RANSOMWARE
   1. MINISTRIES, PUBLIC SECTOR
2. DATA BREACHES
   1. PUBLISHED DATA ON DARK WEB
3. THREATS
   1. REPORTS FOR EXPLOSIVE DEVICES PLANTET IN SCHOOL AND PUBLIC INSTITUTIONS
4. DDoS
   1. BANKS

DISCUSSION POINT: MOST DANGEROUS TYPE OF ATTACK? (10 min)

RANSOMWARE:

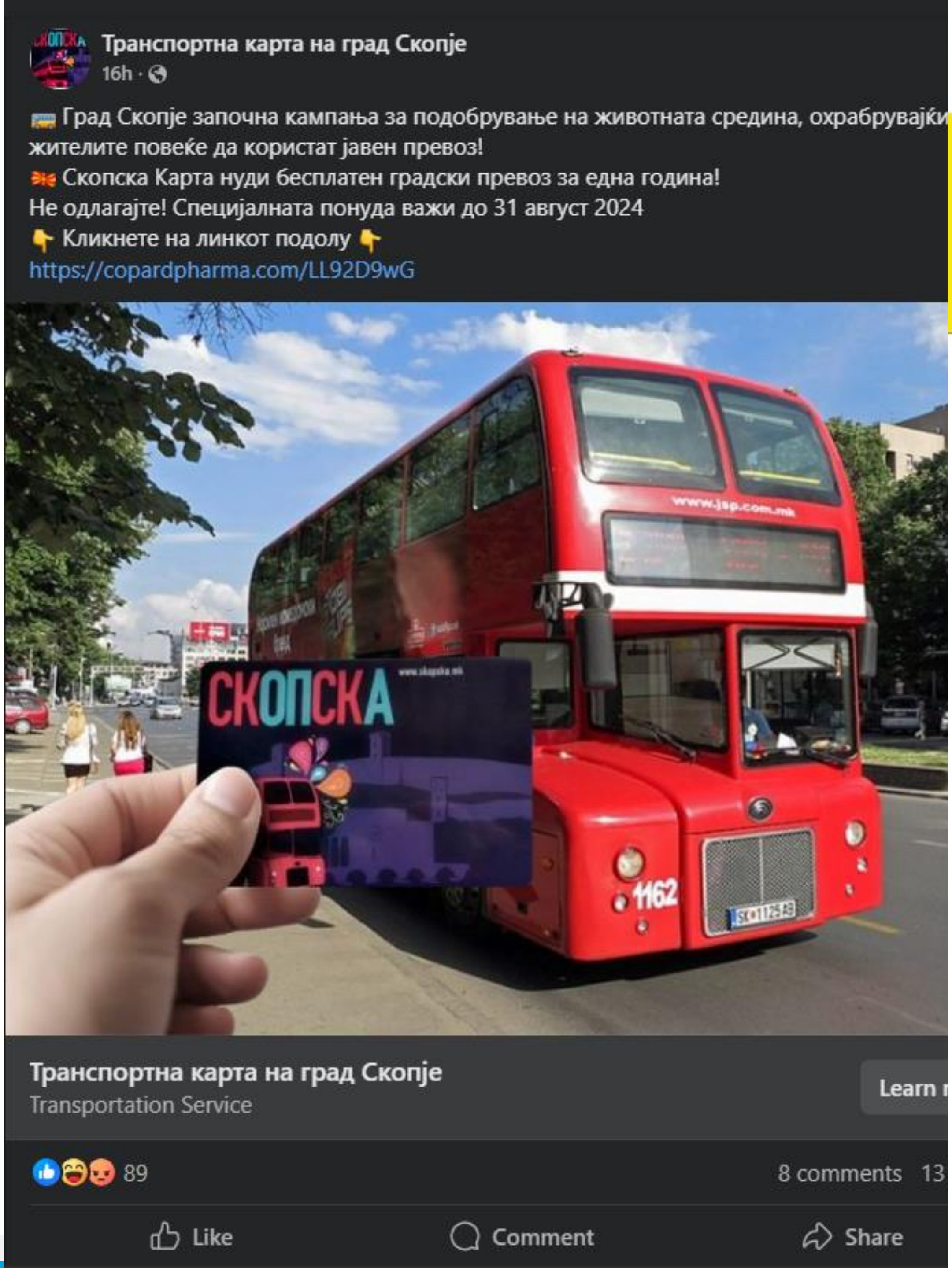
- WHY?
- driven by both opportunity and the value of the data that schools hold


Phishing
Ransomware
Distributed Denial-of-Service Attacks
Video Conferencing Disruptions

HANDS-ON DEMO:

PHISHING EMAILS
RANSOMWARE
ATTACKS

IDENTIFY
REPORT
INVESTIGATE
LEARN
RESILIENCE!!!

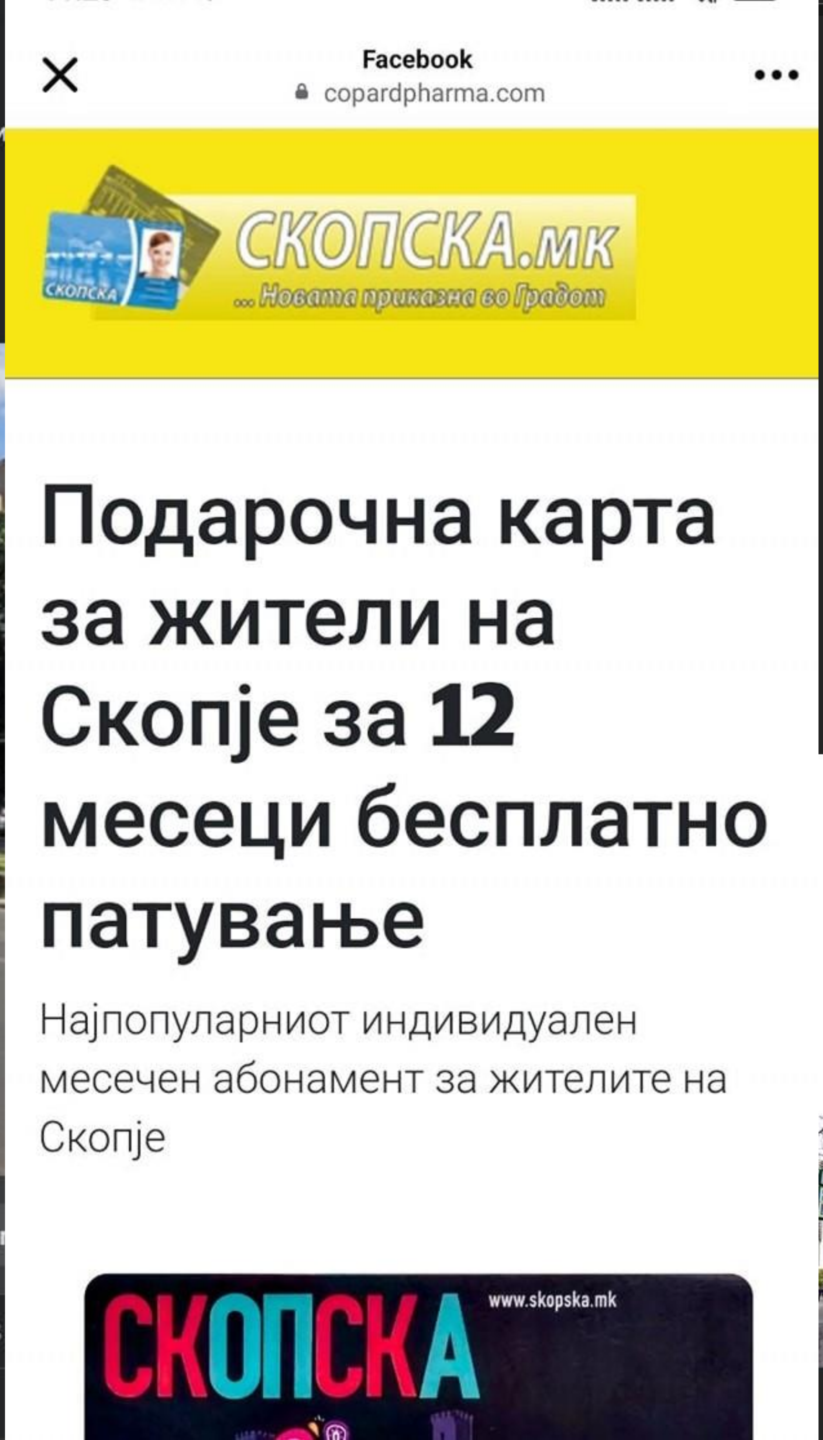


Транспортна карта на град Скопје
16h · 🌐

🚌 Град Скопје започна кампања за подобрување на животната средина, охрабрувајќи
жителите повеќе да користат јавен превоз!
🇲🇰 Скопска Карта нуди бесплатен градски превоз за една година!
Не одлагајте! Специјалната понуда важи до 31 август 2024
👇 Кликнете на линкот подолу 👇
https://copardpharma.com/LL92D9wG

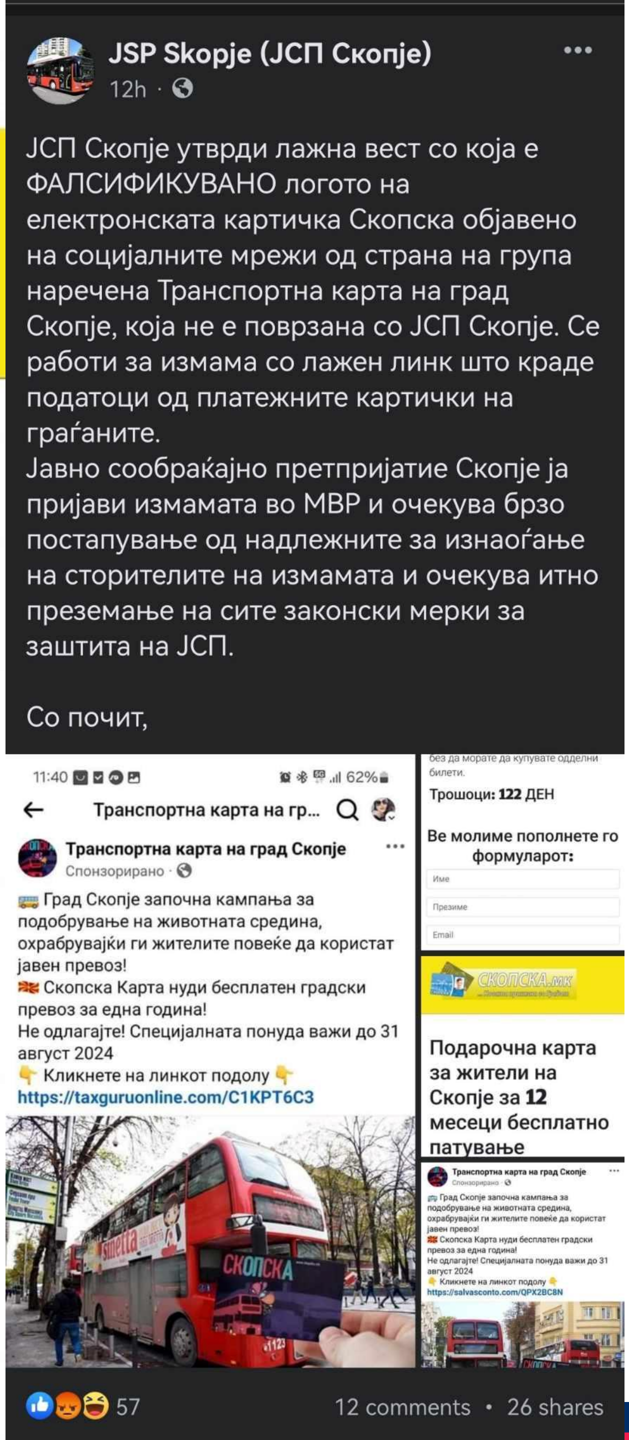
Транспортна карта на град Скопје
Transportation Service

89 · 8 comments · 13



Подарочна карта за жители на Скопје за **12** месеци бесплатно патување

Најпопуларниот индивидуален месечен абонамент за жителите на Скопје



JSP Skopje (ЈСП Скопје)
12h · 🌐

ЈСП Скопје утврди лажна вест со која е ФАЛСИФИКУВАНО логото на електронската картичка Скопска објавено на социјалните мрежи од страна на група наречена Транспортна карта на град Скопје, која не е поврзана со ЈСП Скопје. Се работи за измама со лажен линк што краде податоци од платежните картички на граѓаните.

Јавно сообраќајно претпријатие Скопје ја пријави измамата во МВР и очекува брзо постапување од надлежните за изнаоѓање на сторителите на измамата и очекува итно преземање на сите законски мерки за заштита на ЈСП.

Со почит,

11:40 · 62%

← Транспортна карта на гр...

Транспортна карта на град Скопје
Спонзорирано · 🌐

🚌 Град Скопје започна кампања за подобрување на животната средина, охрабрувајќи ги жителите повеќе да користат јавен превоз!
🇲🇰 Скопска Карта нуди бесплатен градски превоз за една година!
Не одлагајте! Специјалната понуда важи до 31 август 2024
👇 Кликнете на линкот подолу 👇
https://taxguruonline.com/C1KPT6C3

без да морате да купувате одделни билети.

Трошоци: **122** ДЕН

Ве молиме пополнете го формуларот:

Име

Презиме

Email

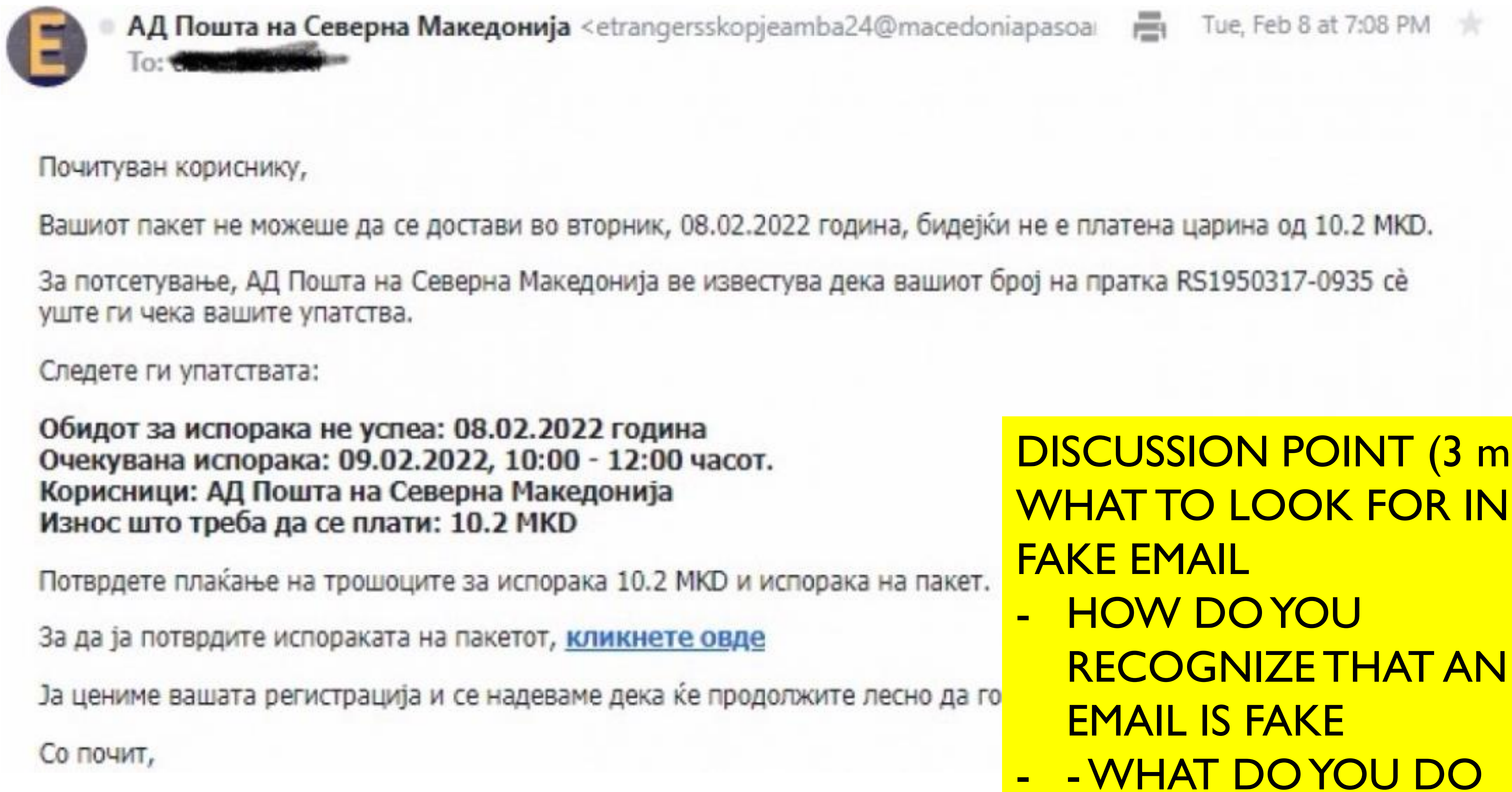
Подарочна карта за жители на Скопје за **12** месеци бесплатно патување

Транспортна карта на град Скопје
Спонзорирано · 🌐

🚌 Град Скопје започна кампања за подобрување на животната средина, охрабрувајќи ги жителите повеќе да користат јавен превоз!
🇲🇰 Скопска Карта нуди бесплатен градски превоз за една година!
Не одлагајте! Специјалната понуда важи до 31 август 2024
👇 Кликнете на линкот подолу 👇
https://salvasconto.com/QPX2BC8N

57 · 12 comments • 26 shares

PHISHING EMAIL DEMO – SPOT THE SIGNS



АД Пошта на Северна Македонија <etrangersskopjeamba24@macedoniapasoa Tue, Feb 8 at 7:08 PM
To: [redacted]

Почитуван кориснику,

Вашиот пакет не можеше да се достави во вторник, 08.02.2022 година, бидејќи не е платена царина од 10.2 MKD.

За потсетување, АД Пошта на Северна Македонија ве известува дека вашиот број на пратка RS1950317-0935 сè уште ги чека вашите упатства.

Следете ги упатствата:

Обидот за испорака не успеа: 08.02.2022 година
Очекувана испорака: 09.02.2022, 10:00 - 12:00 часот.
Корисници: АД Пошта на Северна Македонија
Износ што треба да се плати: 10.2 MKD

Потврдете плаќање на трошоците за испорака 10.2 MKD и испорака на пакет.

За да ја потврдите испораката на пакетот, кликнете овде

Ја цениме вашата регистрација и се надеваме дека ќе продолжите лесно да го

Со почит,

DISCUSSION POINT (3 min)
WHAT TO LOOK FOR IN A FAKE EMAIL

- HOW DO YOU RECOGNIZE THAT AN EMAIL IS FAKE
- - WHAT DO YOU DO

PHISHING EMAIL DEMO – FIND THE REAL SENDER AND CHECK THE ATTACHMENT

EMAIL TRACING

- FIND OUT WHO SEND YOU THAT EMAIL AND FROM WHERE!
- ALWAYS CHECK SUSPICIOUS ATTACHMENTS AND EMAILS

https://www.virustotal.com

DISCUSSION POINT (5 min)

DEMONSTRATION TIME

ANALYZE EMAIL HEADER SERVICE:
https://www.whatismyip.com/email-header-analyzer/
GOOGLE GUIDE ON HOW TO TRACE THE REAL SENDER:
https://support.google.com/mail/answer/29436?hl=en

RANSOMWARE DEMO – WHAT DO YOU DO FIRST?

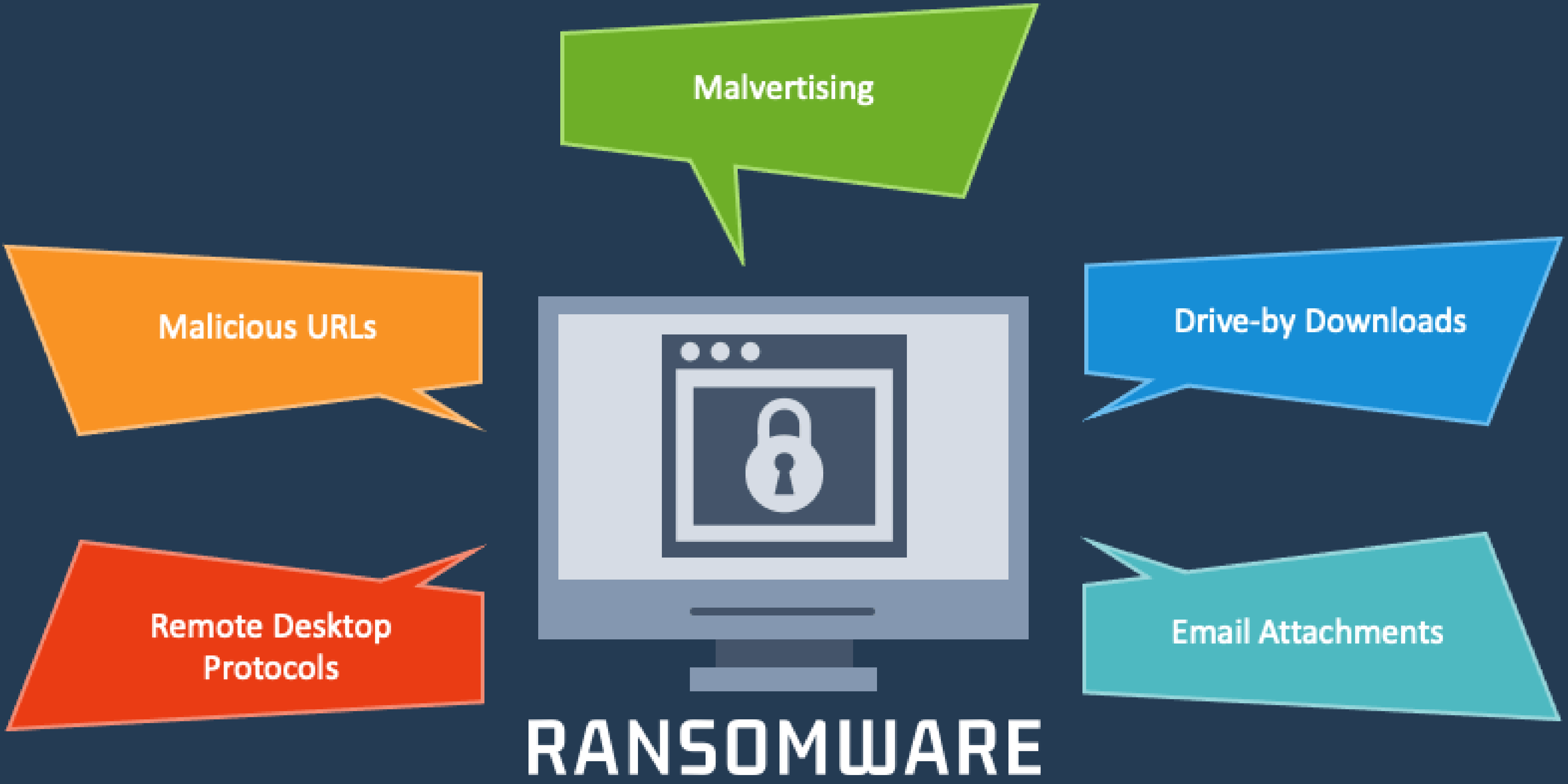
OPTIONS:

1. TURN OFF THE COMPUTER
2. DISCONNECT FROM NETWORK
3. CALL IT SUPPORT
4. CALL SUPERVISOR
5. CALL A COLLEAGUE
6. POST ON FACEBOOK

DISCUSSION POINT (5 min)
HOW RANSOMWARE IS SPREADING

RANSOMWARE

How does Ransomware Spread?



Malvertising

Malicious URLs

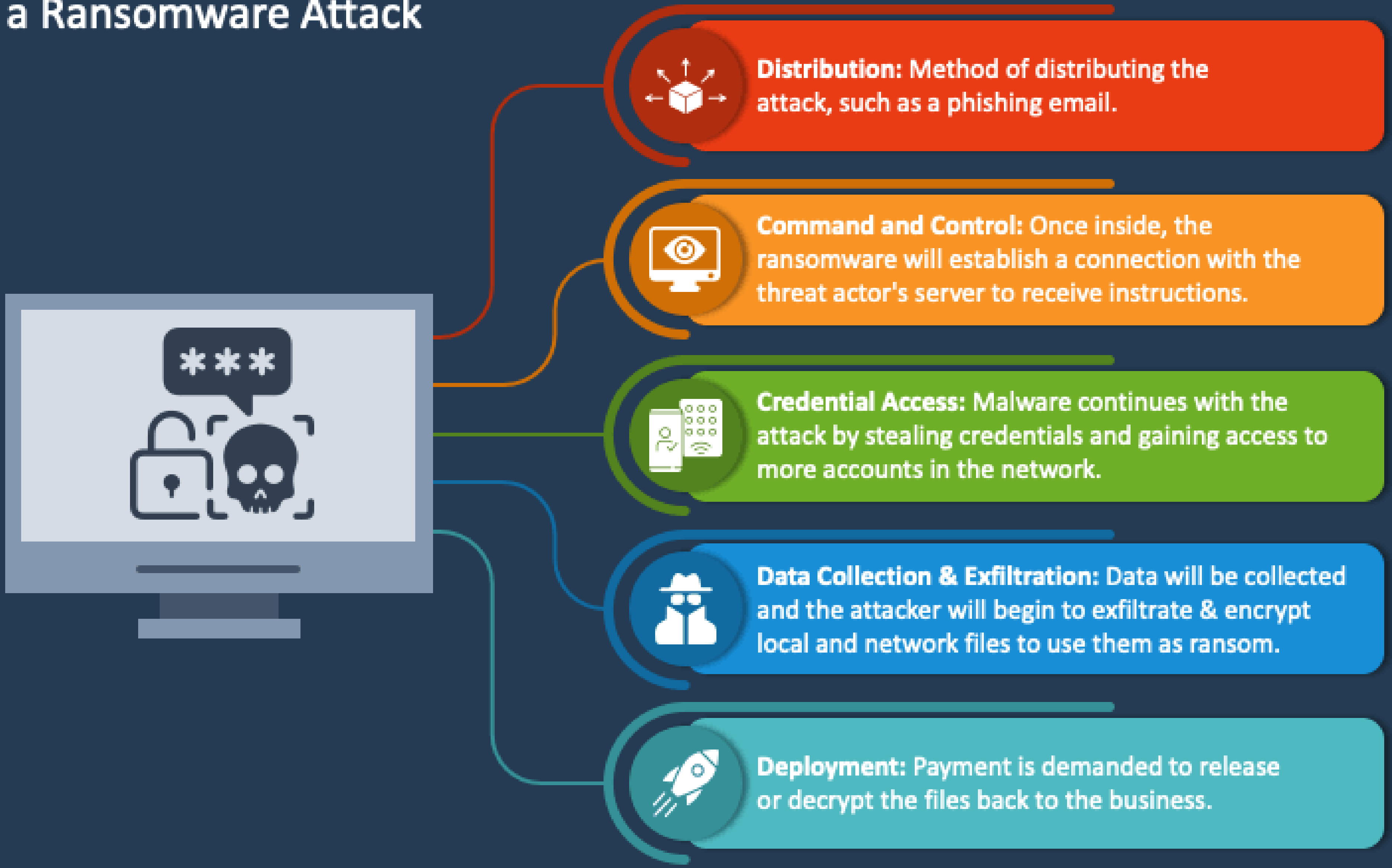
Drive-by Downloads

Remote Desktop Protocols

Email Attachments

RANSOMWARE

Stages of a Ransomware Attack



Distribution: Method of distributing the attack, such as a phishing email.

Command and Control: Once inside, the ransomware will establish a connection with the threat actor's server to receive instructions.

Credential Access: Malware continues with the attack by stealing credentials and gaining access to more accounts in the network.

Data Collection & Exfiltration: Data will be collected and the attacker will begin to exfiltrate & encrypt local and network files to use them as ransom.

Deployment: Payment is demanded to release or decrypt the files back to the business.

CYBERSECURITY AND MISINFORMATION (OR FAKE NEWS)

MAKING INFORMED DECISIONS

CYBERSECURITY AND MISINFORMATION (OR FAKE NEWS)

1. Information Warfare and Cyber Espionage

- **State-sponsored cyber activities:** Some nation-states use cyber capabilities to spread misinformation as part of broader information warfare campaigns. This can be to destabilize political processes in rival countries, influence public opinion, or discredit opposition.
- **Case:** The interference in the 2016 U.S. election, where hackers allegedly linked to the Russian government stole and leaked information, is a notable example. This was not just a cybersecurity breach but also a misinformation campaign to influence public opinion.
- https://www.cisa.gov/rumor-vs-reality

CYBERSECURITY AND MISINFORMATION (OR FAKE NEWS)

CYBERSECURITY AND MISINFORMATION (OR FAKE NEWS)

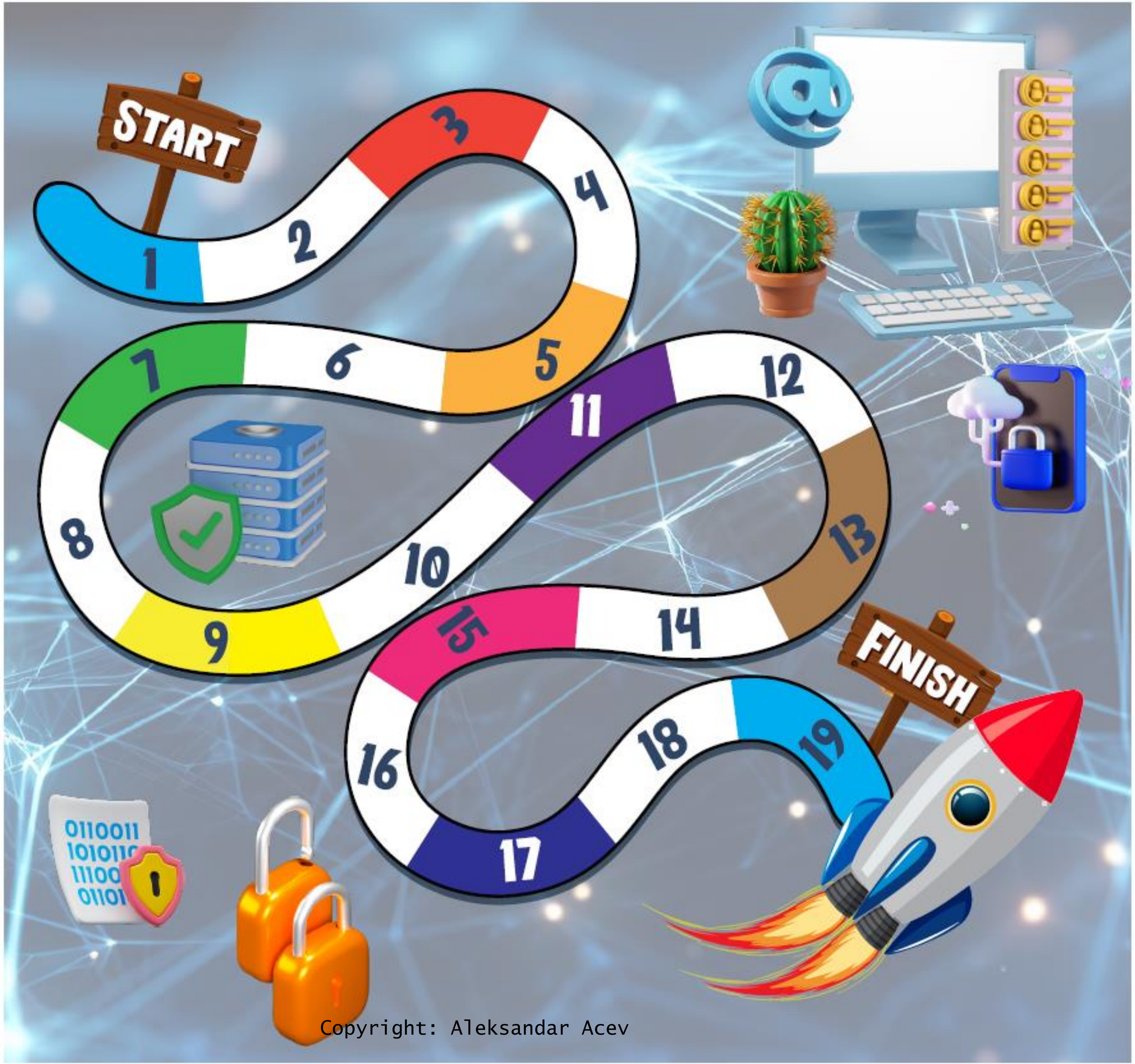
3. Amplification of Misinformation through Botnets

- **Automated spreading:** Cyber attackers can use botnets to amplify misinformation on social media platforms, making it seem more popular or credible than it actually is.
- **Case:** During the COVID-19 pandemic, INTERPOL reported an alarming rate of cyberattacks, with some cases involving misinformation scams via mobile text-messages containing 'too good to be true' offers.
-
- https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

A DAY IN THE DIGITAL LIFE

Demo for board game applicable for teachers and students!

15 minutes



A DAY IN THE DIGITAL LIFE

Objective:

Navigate through a day in the digital life of a teacher, identifying and mitigating potential cybersecurity risks and threats associated with each online activity.

Gameplay:

Players roll the dice and move their token.
Upon landing on an activity space, they draw an Activity Card and read it.
The player then reads the Risk & Threats associated with that card.
The player must choose the correct Mitigation Measure Card.
If correct, they stay;
if not, they move back two spaces.
The first to reach the end while navigating the threats wins.

IDEATE &

PROTOTYPE

ANALYSIS OF AN ATTACK / TTX EXCERCISE

Table Top Exercise – TTX

Cybersecurity Incident in a School

Setting the scene:

- You are a teacher in a primary school.The school has more than 300 students and a staff of 50 people.There are more than 80 PCs. All teachers have their own PC or laptop, or use their private computers for work.The save their files only locally 0 only some of them are trained to use OneDrive to save and sync their files to the cloud.
- There is no backup policy in place, and the endpoint protection licenses have expired 3 months ago. The school does not have dedicated IT support and relies on the good work that the IT teacher is voluntary doing.The secretary is in charge of the administrative activities.

Discussion point (5 min):
What sensitive and important documents and information do YOU keep on your computer?

Table Top Exercise – TTX

PHASE 1: INITIAL DETECTION AND IDENTIFICATION

Inject 1:

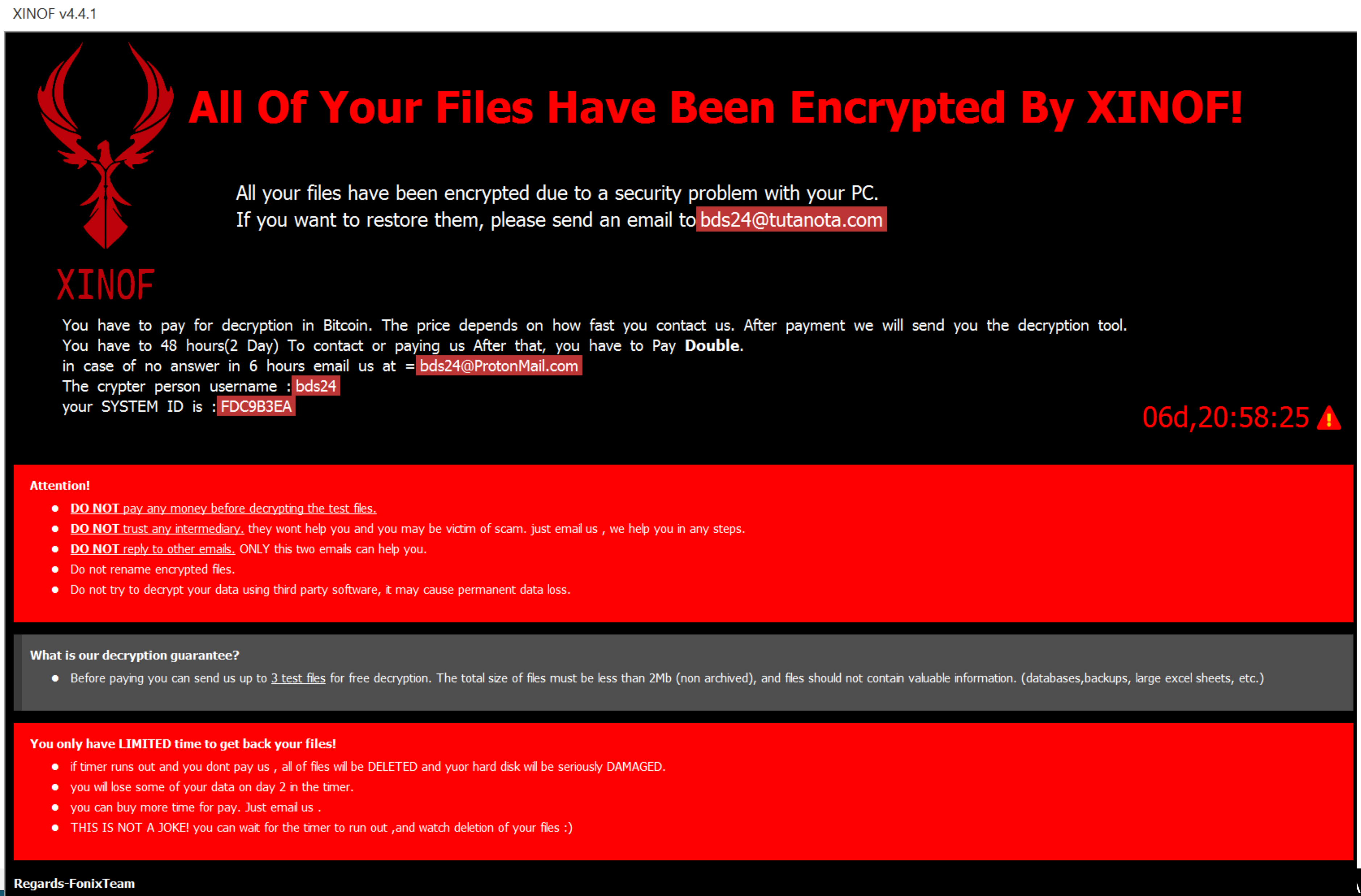
Upon arriving to the school on Monday morning, the school's IT teacher receives multiple reports from other teachers about their computers displaying a ransom note. Simultaneously, an anonymous email is received claiming responsibility for the breach and:

- **demanding a ransom.**
- **Saying the have all student and parents data stolen!**

DISCUSSION POINT (5 MIN):

- **WHO SHOULD THE TEACHER INFORM?**
- **WHAT ARE THE INITIAL STEPS TO BE TAKEN UPON RECEIVING THESE REPORTS.**
- **WHAT WOULD BE THE PROCESS TO VALIDATE AND CONFIRM THE BREACH.**
- **IDENTIFYING AND INFORMING PRIMARY STAKEHOLDERS?**

Example of a Ransomware note - 2



XINOF v4.4.1

All Of Your Files Have Been Encrypted By XINOF!

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email to bds24@tutanota.com

XINOF

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us. After payment we will send you the decryption tool.
You have to 48 hours(2 Day) To contact or paying us After that, you have to Pay **Double.**
in case of no answer in 6 hours email us at = bds24@ProtonMail.com
The crypter person username : bds24
your SYSTEM ID is : FDC9B3EA

06d,20:58:25 ⚠

Attention!

- DO NOT pay any money before decrypting the test files.
- DO NOT trust any intermediary. they wont help you and you may be victim of scam. just email us , we help you in any steps.
- DO NOT reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.

What is our decryption guarantee?

- Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

You only have LIMITED time to get back your files!

- if timer runs out and you dont pay us , all of files will be DELETED and yuor hard disk will be seriously DAMAGED.
- you will lose some of your data on day 2 in the timer.
- you can buy more time for pay. Just email us .
- THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)

Regards-FonixTeam

NoMoreRansom – First place to check for a decryption key

Table Top Exercise – TTX

PHASE 2: CONTAINMENT AND ERADICATION

Inject 2:

The IT teacher receives the report from the expert company that confirms the breach and identifies the ransomware strain. They also discover that the breach originated from a phishing email opened by a staff member.

DISCUSSION POINT (5 MIN):

- **IMMEDIATE ACTIONS TO HALT THE SPREAD OF RANSOMWARE.**
- **STEPS TO VERIFY THE INTEGRITY OF OTHER SYSTEMS.**
- **CRAFTING COMMUNICATION TO STAFF, STUDENTS, AND PARENTS ABOUT THE INCIDENT.**

Table Top Exercise – TTX

PHASE 3: RECOVERY AND COMMUNICATION

Inject 3:

The IT teacher with the support from outside hired IT expert company has isolated the affected systems and begun the recovery process. The school's leadership is considering informing law enforcement and the local community about the breach

DISCUSSION POINT (5 MIN):

- **THE IMPLICATIONS OF INVOLVING LAW ENFORCEMENT.**
- **STRATEGIES TO REASSURE THE SCHOOL COMMUNITY ABOUT DATA SECURITY.**
- **THE ROADMAP TO RESTORE NORMALCY IN OPERATIONS.**
- **DO WE HAVE CONTACTS IN LAW ENFORCEMENT SPECIALIZING IN CYBERCRIMES?**
- **HOW CAN WE TRANSPARENTLY COMMUNICATE THE EXTENT OF THE BREACH TO STAKEHOLDERS?**
- **WHAT IS OUR BACKUP AND DATA RECOVERY PROTOCOL?**

Table Top Exercise – TTX

PHASE 4: LESSONS LEARNED AND FUTURE PREVENTION

Inject 4:

The school has successfully recovered from the ransomware attack without paying the ransom. An external cybersecurity firm was hired to assess the school's cybersecurity posture and provided recommendations.

DISCUSSION POINT (5 MIN):

- **REFLECTING ON THE INCIDENT'S HANDLING AND IDENTIFYING GAPS.**
- **IMPLEMENTING STRONGER CYBERSECURITY DEFENSES.**
- **ENHANCING CYBERSECURITY AWARENESS AMONG STAFF AND STUDENTS.**

- **SHOULD WE CONSIDER A REGULAR CYBERSECURITY AUDIT?**
- **HOW CAN WE INTEGRATE CYBERSECURITY BEST PRACTICES INTO THE SCHOOL CURRICULUM?**
- **WHAT ARE THE RECOMMENDATIONS FROM THE EXTERNAL CYBERSECURITY FIRM?**

Table Top Exercise – TTX

WHAT HAPPENED?

HOW ATTACKERS COMPROMISED THE SCHOOL:

Phishing Email: A seemingly innocuous email was sent to multiple staff members. One staff member, believing the email to be genuine, clicked on a link, inadvertently downloading the ransomware.

Weak Passwords: Some staff members had weak or commonly used passwords, making it easier for attackers to gain unauthorized access.

Outdated Software: The school's systems were running outdated software versions with known vulnerabilities, which the attackers exploited.

Lack of Multi-Factor Authentication (MFA): The absence of MFA allowed attackers to access systems once they had the correct credentials without any additional verification.

Insufficient Network Segmentation: The school's network was not adequately segmented, allowing the ransomware to spread quickly across different departments.

DISCUSSION & PROPOSALS

Thank You

ANY QUESTIONS?

ALEKSANDAR ACEV, CISA,CISM,CEH

✉ aacevs@gmail.com

+389 70279600