CYBERSECURITY AWARENESS TRAINING

May 2024

Presenter: Filip Simeonov

01 Overview of cybersecurity

Introduction to cybersecurity and its importance

02 Hackers and threats

Detailed explanation related to hackers and threats they pose

03 Defending ourselves

Best practices on how to defend ourselves in the digital world

04 Recommendations

Additional resources to enhance the security posture

OVERVIEW OF CYBERSECURITY

- Cybersecurity involves protecting digital systems from unauthorized access or harm.
- It helps organizations by safeguarding their digital assets, preventing data breaches and cyber attacks, ensuring data integrity, confidentiality, and availability, and preserving trust, reputation, and financial stability.

Data Breaches

Number of reported incidents: 2,814.
Number of breached records:
8,214,886,660.

Malicious Software

Average ransomware payout increased
by 89%
24,000 apps were blocked daily
47% of all internet traffic came from bots

Phishing Attacks

Phishing was the leading infection vector
$17,700 was lost every minute
57 % of organizations saw weekly / daily
phishing attempts.

HACKERS AND THREATS THEY POSE!

01 Blackhat Hacker

Unauthorized intruder for malicious purposes, often for personal gain.

02 Greyhat Hacker

Operates between ethical and unethical hacking practices.

03 Whitehat Hacker

Ethical expert enhancing security by identifying vulnerabilities legally.

04 State sponsored Hackers

Government-backed agent conducting cyber espionage or sabotage.

05 Hacktivists

Activists using hacking to promote social or political causes.

06 Script Kiddies

Inexperienced hackers using pre-made tools for simple attacks.

HACKERS AND THREATS THEY POSE!

Social Engineering Attacks

MITM Attacks

Identity Theft

Invoice Fraud

COMMON TYPES OF MALICIOUS SOFTWARE:

Trojan Horse

Deceptive software, disguised as legitimate.

Spyware

Covertly monitors and gathers user data.

Ransomware

Encrypts files, demands ransom for access.

Adware

Displays unwanted advertisements, compromises privacy.

DEFENDING OURSELVES!!

CREATION OF PASSWORDS

Weak Password: "password123"
Do not use common words, birth dates, pet names, etc.

Strong Password: "W$9eL#2a@Xp!"
Using passphrase is a good method too, e.g.
"t0d@yisshining2o24&"

Create Strong Passwords:

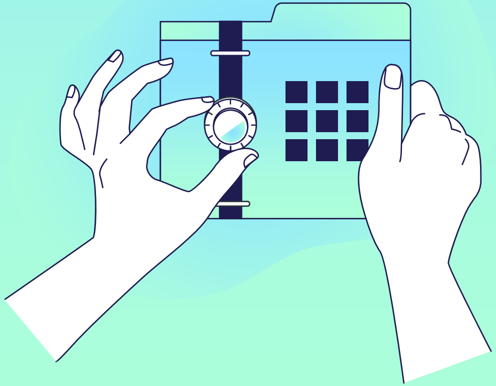
- Use a combination of letters, numbers, and symbols.
- Avoid easily guessable information like birthdays or names.

Unique Passwords for Each Account:

- Don't use the same password across multiple accounts.
- Use a password manager to securely store and manage passwords.

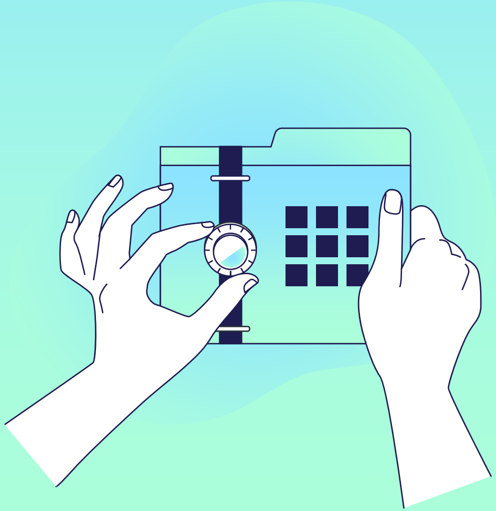
Regularly Update Passwords:

- Change passwords periodically, at least every few months.
- Update passwords immediately if there's a security breach or suspicion of compromise.



STRONG PASSWORD – BETTER SECURITY (EXAMPLES)

“skopjeeglavengrad”	**“Скопје е главен град”**
Bitol@ekonzultskiGr@d	Битола е конзулски град
E.T. Phonehome”	“E-T PhoneHome”
DenesVrneseDozd23!	`Utre’ebideubavovreme@23
TvoiteRusiKosi2010!	Temetoebelosekade341!



DEFENDING OURSELVES!!

AVOIDING SOCIAL ENGINEERING ATTACKS

Be Skeptical of Requests for Information:

- Question unexpected requests for sensitive information.
- Verify the identity of the requester through trusted channels.

Exercise Caution with Email Attachments and Links:

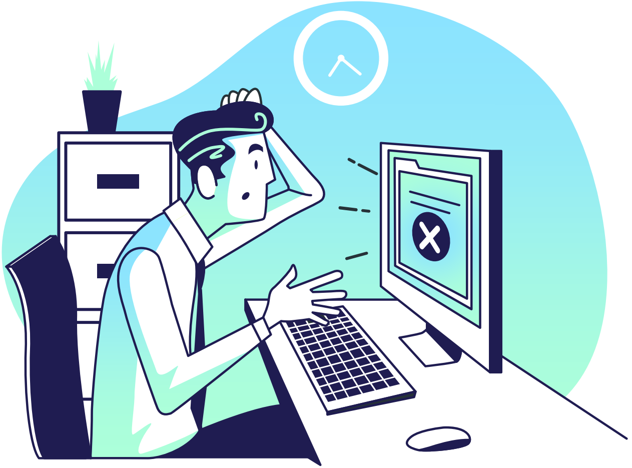
- Avoid opening attachments or clicking on links from unknown or suspicious senders.
- Hover over links to verify the URL before clicking.

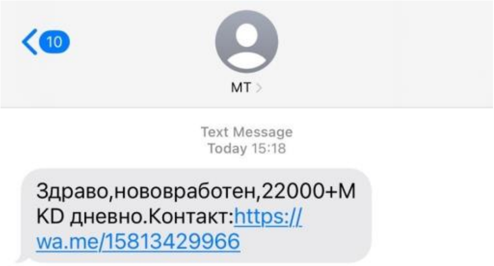
Beware of Urgency or Pressure Tactics:

- Be cautious of requests that create a sense of urgency or pressure to act quickly.
- Take time to verify the legitimacy of the request.

Verify Requests for Financial Transactions:

- Confirm requests for financial transactions through established communication channels.
- Implement dual-authorization processes for sensitive transactions.



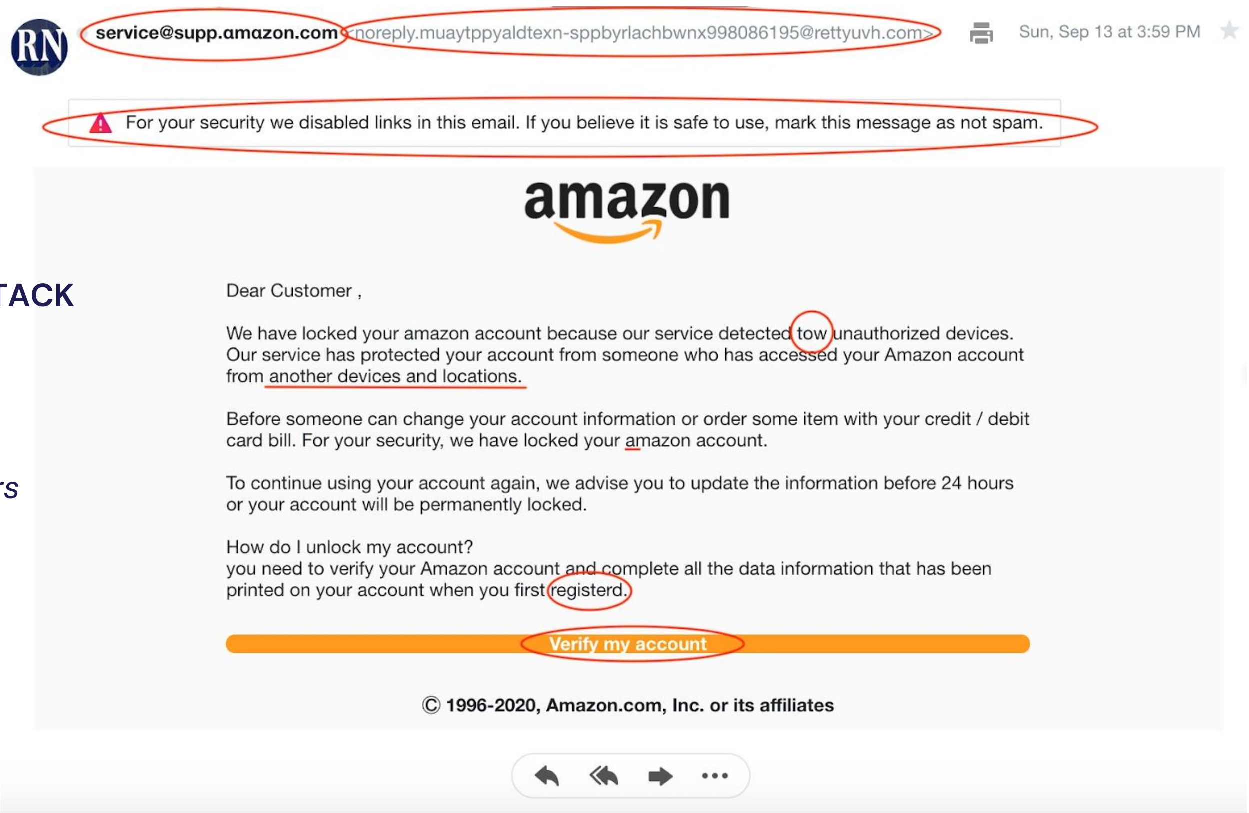


Text Message
Today 15:18

Здраво,нововработен,22000+M
KD дневно.Контакт:https://
wa.me/15813429966

WAYS OF DETECTING A PHISHING ATTACK

- *Check the senders address*
- *Look out for phishing warnings*
- *Check for grammatical errors*
- *Be careful with Latin / Cyrillic letters*
- *Sense of urgency*



service@supp.amazon.com <noreply.muaytppyaldtexn-sppbyrlachbwnx998086195@rettyuvh.com>

Sun, Sep 13 at 3:59 PM

For your security we disabled links in this email. If you believe it is safe to use, mark this message as not spam.

Dear Customer ,

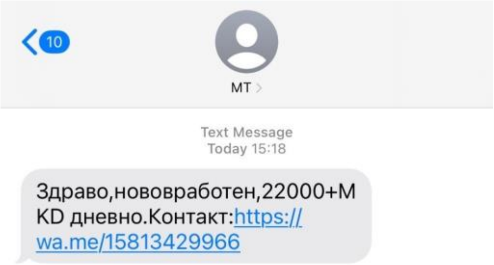
We have locked your amazon account because our service detected tow unauthorized devices. Our service has protected your account from someone who has accessed your Amazon account from another devices and locations.

Before someone can change your account information or order some item with your credit / debit card bill. For your security, we have locked your amazon account.

To continue using your account again, we advise you to update the information before 24 hours or your account will be permanently locked.

How do I unlock my account?
you need to verify your Amazon account and complete all the data information that has been printed on your account when you first registerd.

© 1996-2020, Amazon.com, Inc. or its affiliates



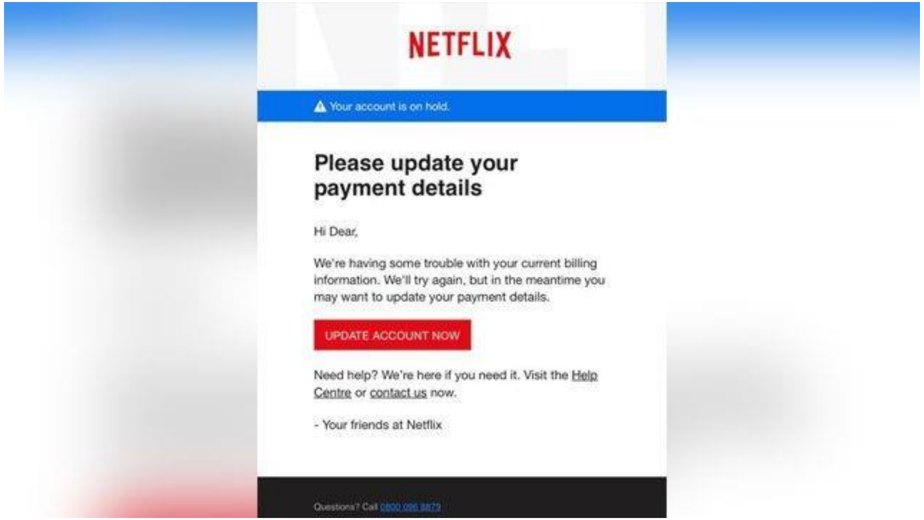
MT

Text Message
Today 15:18

Здраво,нововработен,22000+МKD дневно.Контакт:https://wa.me/15813429966

WAYS OF DETECTING A PHISHING ATTACK

- *Check the senders address*
- *Look out for phishing warnings*
- *Check for grammatical errors*
- *Be careful with Latin / Cyrillic letters*
- *Sense of urgency*



⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 8879

DEFENDING OURSELVES!!

AVOIDING UNTRUSTED NETWORKS

Use Secure Connections (HTTPS):

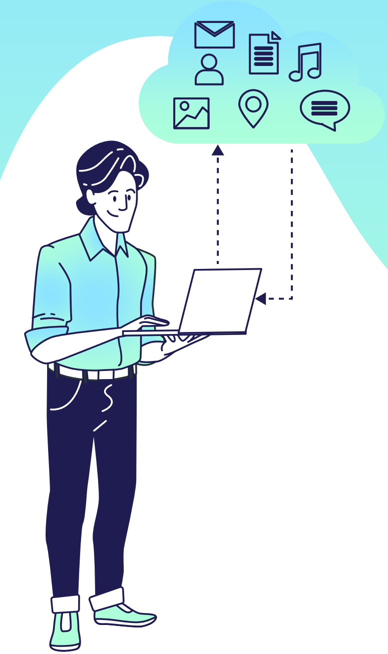
- Access websites using HTTPS to encrypt and protect data transmitted over the network.
- Look for the padlock icon in the address bar to verify a secure connection.

Avoid Public Wi-Fi Networks:

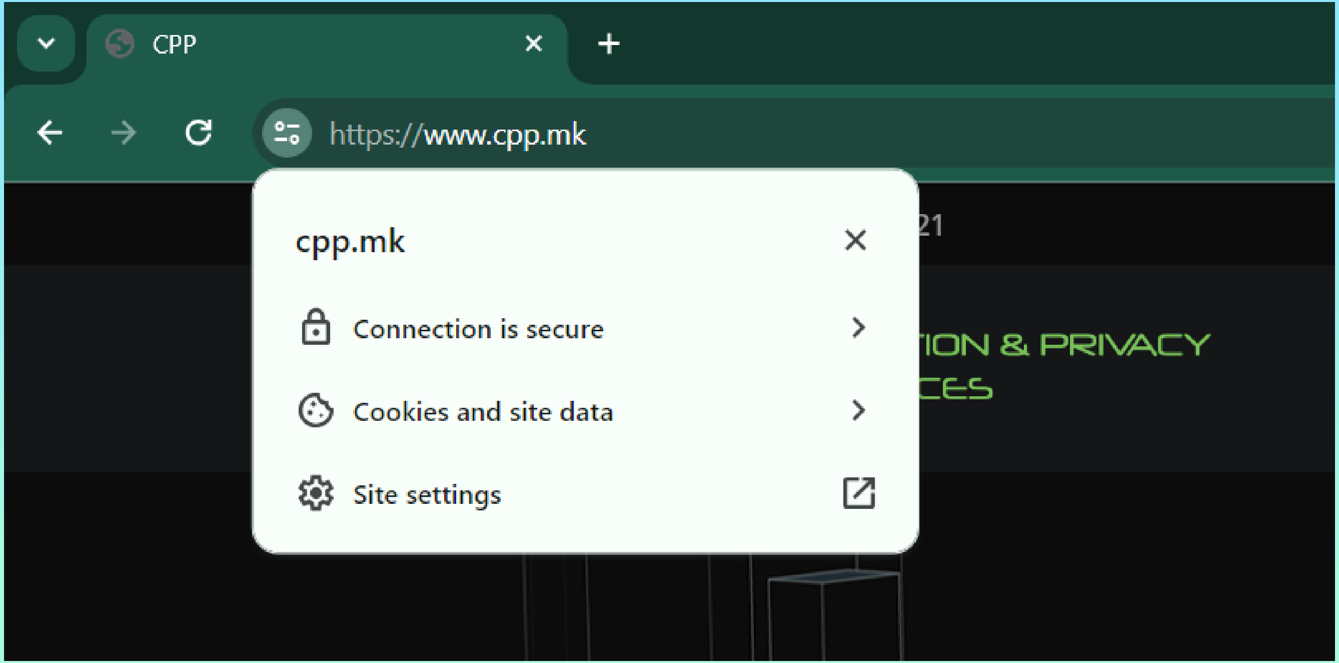
- Limit access to public Wi-Fi networks, especially for sensitive activities like online banking or accessing personal accounts.
- Utilize virtual private networks (VPNs) to protect internet traffic when connecting to public networks.

Verify Network Security:

- Use trusted networks with secure configurations and strong protection protocols (WPA, WPA2, WPA3).
- Avoid networks with weak or no password protection, as they are more vulnerable to interception.



DEFENDING OURSELVES!!



CPP

https://www.cpp.mk

cpp.mk

Connection is secure

Cookies and site data

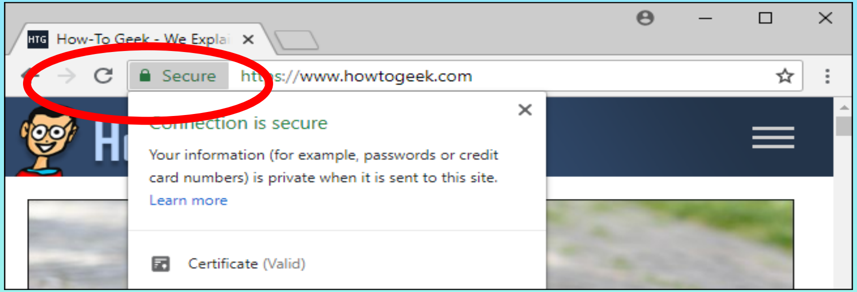
Site settings

21

TION & PRIVACY

CES

DEFENDING OURSELVES!!



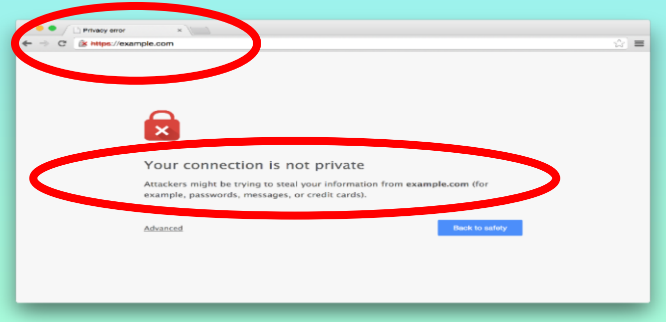
Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)

✓



Your connection is not private

Attackers might be trying to steal your information from **example.com** (for example, passwords, messages, or credit cards).

✗

DEFENDING OURSELVES!!

DON'T SHARE SENSITIVE INFORMATION

Identify Your Personal Data:

- Recognize what information about yourself is sensitive or private.
- Examples include your Social Security number, financial details, and passwords.

Keep Personal Information Private:

- Avoid sharing personal details unnecessarily, especially on public platforms.
- Be cautious when asked for personal information, especially by unfamiliar sources.

Protect Your Online Accounts:

- Use strong, unique passwords for each online account.
- Enable two-factor authentication (2FA) to add an extra layer of security.

Secure Your Devices:

- Set up password protection or biometric authentication on your devices.
- Keep your software and apps updated to patch security vulnerabilities.

DEFENDING OURSELVES!!

IMPORTANCE OF DATA BACKUP

Prevention of Data Loss:

- Backup solutions minimize the risk of losing critical information.
- Business Continuity: Ensure seamless operations by minimizing downtime.

Ensure Data Integrity:

- Quick Recovery: Restore data swiftly after disasters or cyber threats.
- Protection Against Threats: Safeguard data from malware and ransomware.

Compliance and Legal Requirements:

- Data Retention Policies: Adhere to data retention regulations with secure backups.
- Auditing and Accountability: Facilitate auditing and maintain accountability.

Peace of Mind:

- Confidence in Data Availability: Ensure data accessibility whenever needed.
- Risk Mitigation: Minimize financial and reputational risks.

DEFENDING OURSELVES!!

USAGE OF ANTIVIRUS SOFTWARE

Protection Against Malware:

- Malware Detection: Identify and remove harmful software before it can cause damage.
- Prevention of Data Theft: Safeguard sensitive information from being compromised by cybercriminals.

Real-time Threat Detection:

- Continuous Monitoring: Monitor system activities and network traffic for suspicious behavior.
- Immediate Response: Respond promptly to emerging threats to prevent infections and data breaches.

Enhanced Web Security:

- Safe Browsing: Ensure safe navigation by blocking malicious websites and phishing attempts.
- Protection Across Devices: Extend security measures to various devices, including computers, smartphones, and tablets.

System Performance Optimization:

- Resource Efficiency: Utilize system resources efficiently to avoid slowing down the device.
- Scheduled Scans: Perform scans during low activity periods to minimize disruption to users.

DEFENDING OURSELVES!!

UPDATING AND PATCHING

Vulnerability Mitigation:

- Security Vulnerabilities: Address security flaws that could be exploited by cyber attackers.
- Risk Reduction: Minimize the risk of data breaches and unauthorized access to systems.

Improved Performance and Stability:

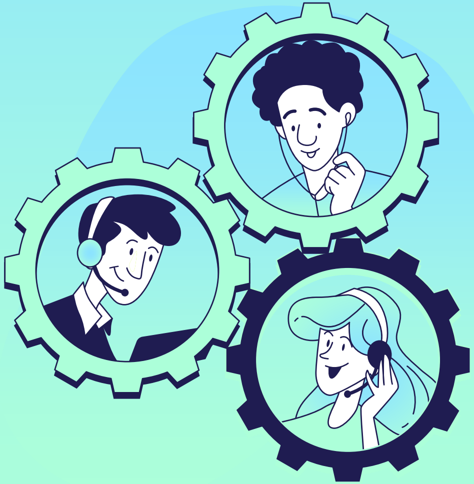
- Optimized Functionality: Ensure software functions are updated and upgraded.
- System Reliability: Reduce crashes and errors by keeping software up to date with the latest fixes.

Compliance Requirements:

- Adherence to Standards: Ensure compliance with industry regulations and organizational policies.
- Data Protection: Protect sensitive data by meeting security requirements outlined in compliance frameworks.

Protection Against Exploits and Malware:

- Mitigation of Exploits: Close security weaknesses to prevent unauthorized access and malware infections.
- Stay Ahead of Threats: Stay one step ahead of cyber threats by proactively addressing known vulnerabilities.



SECURE COMPANY DATA MANAGEMENT

Clear desk policy for safe environment ✓

Confidential data store on safe location ✓

All company data have to be stored on dedicated places ✓

All company data should be printed only in your presence ✓

Forbidden upload and transfer company data through unsecure channels ✓

Forbidden usage of mobile phones and USB for transferring company data ✓

RECOMMENDATIONS

REPORTING

Reporting if anything looks suspicious: Prompt reporting of any suspicious activity or emails is crucial for effective threat mitigation.

ENCRYPTION

Encrypting data adds an extra layer of security, protecting sensitive information from unauthorized access.

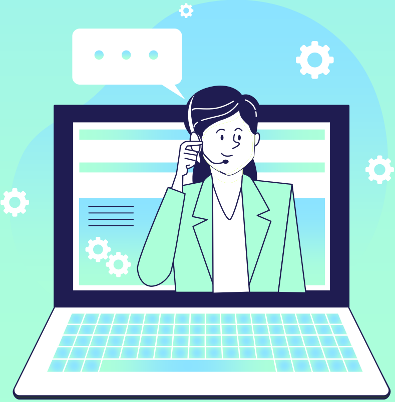
SECURITY AUDITS

Routine audits identify vulnerabilities, ensuring a strong defense against cyber threats and compliance with regulations.

RECOMMENDATIONS

REGULAR AWARENESS TRAININGS

Conducting frequent cybersecurity trainings keeps employees informed and empowers them to make secure decisions.



CONTINUOUS MONITORING

Real-time monitoring enables swift response to security incidents, enhancing overall cybersecurity resilience.

THANKS!

#Becarefull and #staysafe