ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

AN INFORMATION GUIDE

Working From Home

Why are we the targets

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

Why attackers are interested in me?

- Credit card & Financial Data
- Computer Resources
  - Advertising
  - Ransomware
  - Jump point
- User or Email Credentials
  - Sending Spam
  - Recovery/Reset other accounts
  - “More” access
- Medical Data
  - Prescription, insurance, or identity fraud
  - Far more valuable than financial data

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

The Importance of Cybersecurity and Security Technology

Technology alone cannot protect you from everything.
Attackers go where security is weakest.

People are a link in the security chain and the FIRST line of defence.
A MUST to reduce cybersecurity risk.

ncc.cy

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS

COMMISSIONER OF COMMUNICATIONS Digital Security Authority

Co-funded by the European Union

“Home Office”

User Awareness

- Acceptable use of assets
- Intellectual Property of data & assets
- Cybersecurity threats
- Home office security

Endpoint Security

- Corporate endpoint security controls
- User access monitoring
- BYOD
- Mobile Device Management

Internet

VPN Experience & Security

- Capacity management and performance
- Service integrity and availability
- Confidentiality of transmitted data
- User authentication

Stressed-out Third Parties

- VPN provider failure (e.g. DDoS attack)
- Communications provider failure
- Cloud provider performance and availability

Incoming Traffic Security

- Threat awareness and monitoring
- User access management
- Monitoring user activity
- Incident responsiveness
- Security hardening

Corporate Network

IT Internal Infrastructure

- Network segmentation
- Patch & Vulnerability management
- IT change freeze period
- DRP remote access

Outgoing Information

- Data leakage
- Security in transit
- Continuous monitoring
- Email security
- access

Corporate Network

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Discussion points

Key topics covered in this presentation

- Secure your Home Network
- Use a Virtual Private Network [VPN]
- Use strong and unique passwords
- Enable two-factor authentication [2FA]
- Be cautious of phishing attempts
- Encrypt sensitive data
- Backup your data

WHITE

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Secure your Home Network

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with Securing your home network

1. When you setup your router, it often comes with default login credentials. Change the username and password to a strong, unique combination. This prevents unauthorized access to your router's settings.

2. Regularly check for firmware updates from your router manufacturer and install them. These updates often include security patches that address vulnerabilities.

3. Use Wi-Fi Protected Access 2 (WPA2) or Wi-Fi Protected Access 3 (WPA3) encryption protocols on your router. This encrypts the data transmitted between your devices and the router, making it more difficult for attackers to intercept.

4. Set a strong, unique password for your Wi-Fi network. Use a combination of upper and lowercase letters, numbers, and special characters. Avoid using easily guessable information like your name or address.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Securing your home network

1. Check your router settings and disable remote management if it's enabled. This prevents unauthorized access to your router's settings from outside your home network.

2. Most routers have built-in firewalls. Ensure that your router's firewall is enabled to filter incoming and outgoing network traffic. This adds an extra layer of protection against unauthorized access.

3. Review your router's settings and disable any unnecessary services or ports. This reduces the potential attack surface and minimizes the risk of exploitation.

4. MAC address filtering allows you to specify which devices can connect to your network based on their unique MAC addresses. Add the MAC addresses of your trusted devices to the router's whitelist and block any unknown devices.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Last one for Securing your home network

1. Consider setting up separate networks for your work devices and personal devices. This helps isolate your work-related traffic and reduces the risk of cross-contamination.

2. Periodically review the list of devices connected to your network. Remove any unknown or unauthorized devices from the network.

3. If your router supports it, set up a guest network for visitors. This keeps your main network separate and prevents guests from accessing your devices or sensitive information.

4. WPS can be vulnerable to brute-force attacks. Disable this feature on your router to enhance security.

5. Place your router in a central location in your home, away from windows or external walls. This reduces the signal leakage and makes it harder for potential attackers to access your network from outside.

WHITE

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Use a virtual private network (VPN)

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with Using a virtual private network (VPN)

1. A VPN encrypts your internet traffic, making it unreadable to anyone trying to intercept it. This protects your sensitive information, such as passwords, financial data, and personal details, from potential hackers or eavesdroppers on public Wi-Fi networks or insecure connections.

2. A VPN masks your IP address and replaces it with the IP address of the VPN server you're connected to. This helps protect your online privacy by preventing websites, advertisers, or internet service providers (ISPs) from tracking your online activities and collecting data about you.

3. VPNs allow you to bypass geographic restrictions and access content that may be blocked or limited in your location. By connecting to a server in a different country, you can appear as if you're browsing from that location, granting you access to region-specific content, streaming services, or websites.

4. If you work remotely or need to access your company's network from outside the office, a VPN provides a secure connection to your organization's resources. It allows you to access files, databases, or internal systems without compromising security.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Using a virtual private network (VPN)

1 In countries with strict internet censorship or surveillance, a VPN can help bypass these restrictions and access blocked websites or services. It allows users to maintain their freedom of expression and access information without fear of censorship or monitoring.

2 When connecting to public Wi-Fi networks, such as in cafes, airports, or hotels, using a VPN ensures that your data is encrypted and protected from potential hackers or snoopers who may be on the same network.

3 If you engage in peer-to-peer (P2P) file sharing or torrenting, a VPN can provide an extra layer of security. It hides your IP address and encrypts your traffic, reducing the risk of being tracked or targeted by copyright enforcement agencies or malicious actors.

4 By masking your IP address and encrypting your internet traffic, a VPN helps protect your online identity and provides a level of anonymity. This can be particularly important for journalists, activists, or individuals in high-risk environments who need to protect their identities and communications.

WHITE

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Use strong and unique passwords

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with Using strong and unique passwords

1 Strong passwords are harder for attackers to guess or crack through brute-force methods. They typically consist of a combination of uppercase and lowercase letters, numbers, and special characters. This complexity makes it more difficult for hackers to gain unauthorized access to your accounts.

2 Credential stuffing is a common attack where hackers use stolen usernames and passwords from one website to gain unauthorized access to other accounts. By using unique passwords for each account, you minimize the risk of one compromised account leading to a domino effect of breaches across multiple platforms.

3 Many online accounts contain sensitive personal information, such as financial details, addresses, or private messages. Using strong and unique passwords helps protect this information from unauthorized access, reducing the risk of identity theft or fraud.

4 Data breaches are unfortunately common, and they can expose millions of usernames and passwords. By using unique passwords, even if one of your accounts is compromised in a data breach, your other accounts remain secure because the stolen password won't work elsewhere.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Using strong and unique passwords

1 If you use the same password across multiple accounts and one of them is compromised, it can have a negative impact on your professional reputation. For example, if your social media account is hacked, it could lead to unauthorized posts or messages that damage your personal or professional image.

2 Using strong and unique passwords provides peace of mind, knowing that you've taken proactive steps to protect your online accounts and personal information. It reduces the risk of falling victim to cyberattacks and minimizes the potential consequences of unauthorized access.

3 Many organizations and industries have specific password requirements and guidelines to ensure data security. By using strong and unique passwords, you align with these best practices and demonstrate your commitment to maintaining a secure online presence.

4 Remember to regularly update your passwords and avoid reusing them across different accounts. Consider using a password manager to securely store and generate complex passwords, making it easier to maintain strong and unique passwords for all your accounts.

WHITE

ncc.cy

NCC
CYBERSECURITY NATIONAL
COORDINATION CENTRE
CYPRUS

COMMISSIONER
OF COMMUNICATIONS
Digital
Security
Authority

Co-funded by
the European Union

Enable two-factor authentication (2FA)

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with Enabling two-factor authentication (2FA)

1

2FA adds an extra layer of protection to your accounts by requiring a second form of verification in addition to your password. This means that even if someone manages to obtain your password, they would still need the second factor (such as a unique code sent to your phone) to gain access.

2

In the event of a data breach where passwords are compromised, having 2FA enabled significantly reduces the risk of unauthorized access to your accounts. Even if your password is exposed, the attacker would still need the second factor to successfully log in.

3

Phishing attacks involve tricking users into revealing their login credentials on fake websites or through deceptive emails. With 2FA enabled, even if you unknowingly provide your password to a phishing site, the attacker would still be unable to access your account without the second factor.

4

If you frequently access your accounts from different devices or locations, 2FA provides an added layer of security. It ensures that even if someone gains access to your password, they would still need the second factor, which is typically tied to your physical device, to log in.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Enabling two-factor authentication (2FA)

1. Many online accounts contain sensitive information, such as financial data, personal messages, or confidential documents. Enabling 2FA helps safeguard this information by making it significantly more difficult for unauthorized individuals to gain access.

2. In certain industries or organizations, enabling 2FA may be a requirement to meet security standards or regulatory compliance. By enabling 2FA, you demonstrate your commitment to protecting sensitive data and aligning with industry best practices.

3. Enabling 2FA provides peace of mind, knowing that you have taken an additional step to secure your accounts. It adds an extra barrier against unauthorized access and reduces the risk of identity theft, fraud, or unauthorized activity.

4. It's important to note that while 2FA significantly enhances security, it is not foolproof. It's still crucial to use strong and unique passwords, regularly update your software, and practice good online hygiene to maintain a robust security posture.

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Be cautious of phishing attempts

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with phishing attempts

1

Phishing attempts often aim to trick individuals into revealing their personal information, such as usernames, passwords, social security numbers, or credit card details. By being aware of phishing techniques, you can avoid falling victim to these scams and protect yourself from identity theft.

2

Phishing attacks frequently target banking and financial accounts. By recognizing phishing attempts, you can avoid providing your login credentials or other sensitive information to fraudulent websites or individuals. This helps protect your financial accounts from unauthorized access and potential financial loss.

3

Phishing emails or messages may contain malicious attachments or links that, when clicked, can install malware on your device. By being aware of phishing attempts, you can avoid clicking on suspicious links or downloading malicious files, reducing the risk of malware infections that can compromise your device's security and privacy.

4

Phishing attempts often involve tricking individuals into revealing personal information that can be used for various purposes, including targeted advertising or unauthorized access to your online accounts. By staying aware of phishing techniques, you can protect your online privacy and limit the amount of personal information shared with malicious actors.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with phishing attempts

1

Phishing attacks can also target businesses, attempting to gain access to sensitive company data or compromise employee accounts. By being aware of phishing attempts, you can help protect your organization's confidential information and prevent potential data breaches.

2

Falling victim to a phishing attack can have negative consequences for your personal or professional reputation. By being aware of phishing attempts and avoiding becoming a victim, you can maintain your reputation and prevent potential damage caused by unauthorized access to your accounts or dissemination of false information.

3

Many organizations have security policies in place that require employees to be aware of phishing attempts and report any suspicious activity. By staying vigilant, you contribute to maintaining a secure environment and complying with security protocols.

4

Remember to regularly educate yourself about the latest phishing techniques, be cautious when interacting with emails or messages from unknown sources, and report any suspicious activity to the appropriate authorities or your organization's IT department. By being aware of phishing attempts, you can significantly reduce the risk of falling victim to these scams and protect your personal and financial information.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Encrypt sensitive data

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with Encrypting sensitive data

1 Encryption converts your sensitive data into an unreadable format that can only be deciphered with the correct encryption key. This ensures that even if someone gains unauthorized access to your data, they won't be able to understand or use it without the encryption key.

2 Many industries and jurisdictions have specific data protection regulations that require the encryption of sensitive information. By encrypting your data, you can ensure compliance with these regulations and avoid potential legal and financial consequences.

3 Encryption helps protect personal and financial information, such as social security numbers, credit card details, or medical records. In the event of a data breach or unauthorized access, encrypted data remains secure and unusable to attackers.

4 When transmitting sensitive data over networks or the internet, encryption provides an additional layer of security. It prevents eavesdroppers or hackers from intercepting and understanding the data as it travels between devices or systems.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Encrypting sensitive data

1 In the event of a physical theft or loss of devices containing sensitive data, encryption ensures that the data remains protected. Without the encryption key, the stolen or lost device becomes useless to unauthorized individuals.

2 Encrypting sensitive data demonstrates a commitment to data security and privacy. It helps build trust with customers, clients, or partners who rely on your organization to protect their information. This can enhance your reputation and differentiate you from competitors.

3 Encrypting sensitive data provides peace of mind, knowing that even if your data is compromised, it remains secure and unusable to unauthorized individuals. It adds an extra layer of protection and reduces the potential impact of data breaches or unauthorized access.

4 Remember to use strong encryption algorithms and secure encryption keys. Regularly update your encryption software or protocols to ensure you're using the latest security standards. Additionally, consider encrypting data at rest (stored on devices or servers) as well as data in transit (being transmitted between systems) for comprehensive protection.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
WHITE Digital Security Authority

Co-funded by the European Union

Backup your data

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

WHITE

Lets get Familiar with Backing-up your data

1 ZAccidental deletion, hardware failure, or software errors can result in the loss of important data. Regular data backups provide a means to restore lost or deleted files, ensuring that you can recover your data and minimize the impact of such incidents.

2 Data corruption can occur due to various reasons, including malware infections or hardware malfunctions. Regular backups help protect against data corruption by providing clean copies of your files that can be restored. In the case of ransomware attacks, where your data is encrypted and held hostage, having backups allows you to restore your data without paying the ransom.

3 In the event of a natural disaster, fire, theft, or other catastrophic events, data backups are crucial for business continuity. They enable you to recover your critical data and resume operations quickly, minimizing downtime and potential financial losses.

4 Many industries and jurisdictions have specific data protection regulations that require organizations to have backup and recovery mechanisms in place. By implementing data backups, you can ensure compliance with these regulations and avoid potential legal and financial consequences.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with Backing-up your data

1 Data backups help protect your intellectual property, proprietary information, and valuable business data. Losing such data can have severe consequences for your organization's competitiveness, reputation, and overall success. Regular backups ensure that your valuable information is securely stored and can be recovered if needed.

2 Knowing that your data is backed up provides peace of mind, reducing anxiety about potential data loss or system failures. It allows you to focus on your work or business without worrying about the consequences of data loss.

3 Data backups simplify the process of migrating data to new systems or upgrading existing ones. They ensure a smooth transition by allowing you to transfer your data to new hardware or software environments without the risk of data loss or corruption.

4 Remember to regularly test your backups to ensure their integrity and reliability. Store backups in secure locations, both on-site and off-site, to protect against physical damage or theft. Additionally, consider using a combination of local backups and cloud-based backup solutions for added redundancy and protection.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Do you have any questions?