Module B209: Cyber hygiene for Workers

Module B209:
Cyber hygiene for Workers

CYBERHYGIENE FOR WORKERS
Learning Outline

Course outline

- Introduction to Cyber Hygiene for Workers
- Cyber Hygiene for Your Device
- Securing Access to Devices and Services
- Cyber Hygiene for Social Media and Messaging

- Connectivity Cyber Hygiene
- .Email Security
- Keeping Money Safe Online
- Safe Online Shopping and Banking:
- 9.Guidance for People Living with Disabilities
-

Learning Outcomes

1 : Cyber hygiene for workers

1.1: Value and importance of cyber hygiene for workers

1.2 Recognizing common cyber threats and risks to personal, work data and applications

What is cyber hygiene for workers?

- Workers in various sectors interact with various resources including hardware, software, applications, data and information and user credentials that should be protected from compromise.

- Cyber hygiene for workers help to:
- Learn the risks posed to various resources at their access by cybercriminals,
- Learn the implications of a cyber breach and
- Learn subsequent measures and best practises to engage and protect them.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT technology transforming lives

Value and importance of cyber hygiene for workers

Cyber hygiene focuses on

- Enhancing best practices in user behaviors
- Securing resources from unauthorized use and compromise
- Protect sensitive information from cybercriminals and hackers
- Maintain online security and privacy
- Minimize and mitigate the risk of cyberattacks
- Protect organizations from financial losses

Common Cyber Hygiene problems

- **Advancing attack methods** and complexity by cybercriminals
- **Workers buy-in** – security measures need the integration of various users and their experiences
- **Security breaches** – Failure to install and update security applications and patches
- **Failure to protect against cyber threat** leaving workers exposed to vulnerable that hackers

- **Data loss** – hard drives failure and cloud compromise
- **Data loss for lack of backups**
- **Vulnerable back media** / location
- Use of older legacy applications
- Increased phishing scams
- Lack of cyber hygiene awareness

Benefits of Cyber Hygiene for workers

Basics of cyber- hygiene workers include

- Maintain security for the systems in your digital space
- Understand and protection against cyber threats such as malware, phishing attacks, and hacking attempts.
- Help mitigate of damage from cyberattacks – Even with good cyber hygiene, cyberattacks can still occur. However,
- Protect against financial losses (fines and litigations for non-compliance and recovery)
- Protect against damage to reputation when compromised.
- Protection against data and identity theft

Practices for cyber hygiene for workers

- Protect resources against cyber threats
- Regularly update software and applications using strong passwords
- Avoid clicking suspicious links and attachments – they install applications1
- Infuse good password practises – prevent against password attacks
- Protect devices - this reduces the attack surface and risks of compromise.
- Compliance with regulations - demonstrates hygiene practices
- Minimise avoid potential penalties.

Cost savings

- Reduced downtime, productivity and cost of replacing hardware
- Reserves company image due to good reputation and compliance
- Invest in good cyber hygiene practices for workers saves the organization money by avoiding the costs of remediation, loss of revenue, fines and reputational damage.

Cyber Hygiene Best Practices

Cyber hygiene best practises include:

- Regularly update device software and applications
- Hardware updates prevent performance issues
- Manage your passwords hygiene
  - Create strong and secure passwords I
  - Implement Multi Factor Authentication

Multi Factor Authentication - MFA

- Breaks series of attempted password attacks by providing and additional layer of authentication send to the account holder via:

i. **Something you know**
   Pin or Password, answer
ii. **Something you have**
   -card or phone, finger print
iii. **Something you are**
   - user

Cyber Hygiene Best Practices (cont)

- Regularly backup important files / data
- Educating yourself and others
- Review your email browser safety
- Monitoring your account activity
- Unsubscribe to limit data exfiltration
- Create secure backups
- Monitor and report suspicious activity
- Compliance with various regulations and standards
- Business continuity and increased productivity
- Educate yourself and on security trends
- Encryption – implement encryption policies




Cyber Hygiene Best Practices (cont)

- Security software and Firewalls
- Review your online digital interactions - workers
- Implement whitelisting/blacklisting applications, websites and email addresses
- Manage access control
- Avoid falling for phishing Email scams
- Access Safe Websites with the protocol "https" to determine if a website is safe.
- Close Tabs to Prevent Tab napping – workers should avoid opening several unnecessary tabs
- Work Only on Company Devices
- Connect to secure networks only
- Hide Screens whenever in public places

Key risks in cyber hygiene and devices

Key risks include

- Malware attacks
- Hackers
- Bring your own device approach
- Malicious insider threats
- Loss / theft of data
- Password Theft and attacks
- Social engineering attacks
- Zero-Day Exploits
- Attribution
- Non-Compliance and violation of policies
- Drive by download attacks

Devices may be rooted and compromised by malware or other networks

- Devices may be lacking antivirus protection
- Unsupported legacy device hardware platforms with vulnerabilities

Introduction to malware

- malware is a combination of two words; malicious software.
- It's software designed to find a vulnerability in a system and exploit, infect it or disrupt computer operations, access or gather sensitive information for some private

MITIGATION

- Safeguard Your Information – do not share or save PII data online or with everyone
- Review your security posture - conduct Background Checks on yourself
- Create and implement policies and procedures for information security
- Understand work from home policies and protect from compromise.
- Identify and report malicious emails and other activities
- Understand the risk of pop ups and block them
- Disable use of protocols like remote desktop
- Disable use of administratively privileged accounts a-use standard
- Secure your devices, wireless access point and
- Always log out from on line accounts
- Use encryption for sensitive business information

Train your employees in security matters including:

- How to identify security threats and attempts
- secure their personal accounts, devices and applications and social media
- Understand the security risks posed by using removable
- Avoid downloading and installing files and applications from unwarranted sources online
- Review privacy settings in their accounts
- Basic antivirus can protect against some malwares, but a multi-layered security solution that uses antivirus, deep-packet inspection firewalls, intrusion detection systems (IDSs), email virus scanners, and employee awareness training is needed to provide optimal protection
- Undertake security and cyber hygiene training
- Regularly patch and update your systems and applications

For windows users, use the following steps to check the security status of your device:

To customize how your device is protected with these Windows Security features select **Start** > **Settings** > **Update & Security** > **Windows Security** or select the button below.

Open Windows Security settings

Status icons indicate your level of safety:

- **Green** means there aren't any recommended actions right now.
- **Yellow** means there is a safety recommendation for you.
- **Red** is a warning that something needs your immediate attention.

Steps to run a quick scan

1. Select **Start** > **Settings** > **Update & Security** > **Windows Security** and then **Virus & threat protection**.

   Open Windows Security settings

2. Under **Current threats**, select **Quick scan** (or in early versions of Windows 10, under **Threat history**, select **Scan now**).

If the scan doesn't find any issues, but you're still concerned, you may want to check your device more thoroughly.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

1. Select **Start** > **Settings** > **Update & Security** > **Windows Security** and then **Virus & threat protection** > **Manage settings**. (In early versions of Windows 10, select **Virus & threat protection** > **Virus & threat protection settings**.)

   Open Windows Security settings

2. Switch the **Real-time protection** setting to **Off** and choose **Yes** to verify.

2. CYBER HYGIENE FOR YOUR DEVICE

- Upon completion of this module, the participants will be able to:
  - Understanding Devices
  - Key Risks
  - Device Cyber Hygiene Practices
  - Cyber Hygiene on Shared Devices
  - Using Cyber cafes
  - Emerging Technology for Device Cyber Hygiene
  - Key Cyber Hygiene Messages for Devices

Understanding Devices

- **Introduction**
- Shared devices refer to physical or virtual computing resources used by multiple users , individuals or entities across a larger open workspace
- accessed by various technologies and networks to offer various services.
- Shared devices include public computers, shared workstations, or even IoT devices in a home network, are susceptible to various cyber risks.
- These risks can compromise the security and privacy of users who utilize these devices.
- The devices are provisioned to handle high volumes of traffic depending on their types, purposes and desired performance and thresholds.
- Shared devices are intended to offer accessibility to services to may users from a single point and cut costs of buying several devise and applications.
- Key Cyber Hygiene Messages for Devices

Understanding Devices

Common Types of Shared Devices:

- **Public Computers in** libraries, internet cafes, or shared workspaces
- **Kiosks: Touchscreen** kiosks at airports, malls, hospitality institutions or information centers provide information and services to users like government services.
- **Shared Workstations workstations used by multiple employees or shift workers and guests.**
- IoT Devices are configured to share information
  - Smart home devices like thermostats, smart speakers, and security cameras may be shared among family members in a household.
- Virtual Machines: Virtual machines (VMs) and cloud instances can be used by multiple users for various computing tasks.

Key Cyber Hygiene risks of shared devices

- Workers access resources on shared devices at their personal discretion with versions of applications and configuration features in terms of security. These cannot be provisioned for security enhancement and pose a risk to the shared devices in case of compromise.
- Devices dedicated to BYOPD corporate policies may also be handled by many users with varying activities
- Data Theft: Unauthorized users can compromise devices and steal sensitive information left on the device, such as login credentials, personal documents, or financial data.
- Malware Infections: Shared devices can become infected with malware.
- Account Compromise: user login credentials on a shared device can be easily compromised for users who don’t log out or have saved their login credentials on to the devices.
- Email and Phishing Attacks: these are commonly delivered through browsing phishing content downloaded onto shared devices where some workers fall for the trick and compromises by cyber criminals.
- Privacy Concerns: Shared devices may not have strong privacy measures in place
- Inadequate Security Updates
- Physical Security Risks: Shared devices in public spaces are vulnerable to physical tampering or theft,
- Unauthorized Access: improper access control implementation
- Data Residue: these area remnants of data left on the device after a user logs

Mitigating common cyber risks associated with shared devices:

- Workers should identify the resources provisioned for their access and manage their access control permissions
- Limit privilege escalation by using the guest accounts.
- Restrict user activities and permissions on the device and the roles of the workers.
- Use Secure Browsing - prevent the retention of browsing history and data
- Avoid Storing Sensitive Information on line
- Regularly Update and Patch software applications and browsers
- Train and Educate Users in security on the trends of cyberattacks

Device Cyber Hygiene Practices

- Implement Security Software: Use advanced antivirus and anti-malware software
- Secure devices from Physical Access
- Data Encryption: Use encryption tools to protect data
- Manage the computer hardware behaviour and ensure - do not tamper with all parts of a
- Ensure that all software is provisioned for easy access and use by workers
- Do not tamper with user files left - may be intentionally placed for your interaction.
- Always provision guest accounts for guest users

Device Cyber Hygiene Practices

- Be Cautious with Public Wi-Fi - Use a virtual private network (VPN) to encrypt internet connection and protect you
- Stay Updated and patch operating system, software, and apps
- Use reputable security software with advanced capabilities
- Review URLs and Links: Be cautious when interacting with links and shared files for downloading
- Educate in security and cyber hygiene
- Lock your account on the Device
- Report Security Issues
- Physical Security: be mindful of the physical security
- Data Sanitization: If you download or save files , delete them after use

Cyber Hygiene on Shared Devices

- Maintaining good cyber hygiene when using shared devices is essential to protect your privacy and security. Here are some best practices to follow when using shared devices:
- Use Guest Accounts: Whenever possible, use guest or temporary accounts on shared devices. This limits your access to the device's settings and minimizes the risks associated with your session.
- Log Out: Always log out of your accounts
- Clear Browsing Data: After each session, clear your browsing history, cookies, and cached data to remove any traces of your online activity.
- Use Private Browsing Mode
- Use Strong, Unique Passwords for accounts on a shared device,
- Enable Two-Factor Authentication (2FA): Whenever possible, enable 2FA on your accounts to provide an extra layer of security, even if someone gains access to your login credentials.
- Be Cautious with Public Wi-Fi: If you're using a shared device on public Wi-Fi, be cautious. Use a virtual private network (VPN) to encrypt your internet connection and protect your data from eavesdropping.
- Stay Updated: Ensure that the operating system, software, and apps on the shared device are up to date. Keep them patched with the latest security updates.

Using Cyber cafes

- A cyber café is an establishment of computers with internet connection for use by the public to access internet services and other related technology services at a fee. The computers in a cyber café are equipped with various software, including web browsers, office applications, and communication tools for various user needs.
- **A cyber café offers the following services**
- Cyber cafes primarily offer internet access to customers – this include internet browsing, email communication and collaboration services, access online resources and common e-government services using the cafe's computers.
- Computer Usage for a specified period, typically charged on usage.
- Typing, photocopying, printing and scanning services for customers with documents, photos, or scan documents to digital formats.
- Online Gaming and entertainment
- Software and Application Installation for users

Using Cyber cafes- cont

- Purchase of stationery for personal use
- Files download and transfer to removable storage media and devices.
- Technical Support: Cyber cafes may offer basic technical support to assist customers with issues related to internet connectivity, computer usage, or printing.
- Charging Stations for electrical and electronic devices like mobile phones and smartphones and any other electronic devices.
- Webcams and Headphones for participation in teleconferencing services in meetings, online gaming, or other audio-visual needs.
- Modern cyber cafes offer snacks, beverages, and seating areas, creating a relaxed environment for customers to enjoy while using the internet on their devices.
- Educational Services: Cyber cafes may provide educational resources and classes, such as computer training, language learning, or job search assistance.
- Conference, online learning centres and Meeting Rooms
- Other Online Services like doing applications filling online forms, making online reservations, or accessing government digital services.

2.6 : Emerging technologies for enhancing device cyber hygiene

- Secure Boot and Firmware Integrity Verification
- Machine Learning
- Device Patching and Updates Automation
- Artificial Intelligence
- Block chain technology
- Zero Trust Architecture)
- Homomorphic Encryption
- IoT Security Solutions:
- IoT Security Solutions
- Block chain technology
- User and Entity Behavior Analytics (UEBA)
- Multi-Factor Authentication (MFA)
- Secure Access Service Edge (SASE):
- 5G Network Security
- Quantum-Safe Cryptography
- Security Information and Event Management (SIEM

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

3: SECURING ACCESS TO DEVICES AND SERVICES




Device security

- Device security is the process of securing a user's or corporate mobile phones, laptops, PCs, and Internet of Things (IoT) devices from cyber threats and unauthorized access by cyber criminals by implementing strong authentication mechanisms for users, devices and restricted access to network access.
- **Common reasons for device security include:**
- 1. Secure your small home office when working remotely from home by locking the office.
- 2. Establishing zone areas for work and home devices when working from home to manage and access to sensitive data and files.

Device security practises

- Encrypt your devices – implement integrity of data resources and reduces the security risk on lost or stolen devices.

- Ensure your machine has antivirus that is updated
- Disable your notification popups
- Disable "Remember Me" options and let the computers forget you after you log out – checking option bypasses the need to use MFA for subsequent logins for 30 days.

Clear data and files from any devices before you transfer them to another user.

Keep your operating system up to date to beat effort by cybercriminals and rogue applications from accessing and misusing your device.

Factory set mobile phone devices to prevent data from being restored after you stop using the device. To access the reset to factory setting:

Enable the find my device and remote wipe facilities embedded in your device anti malware application and email features.

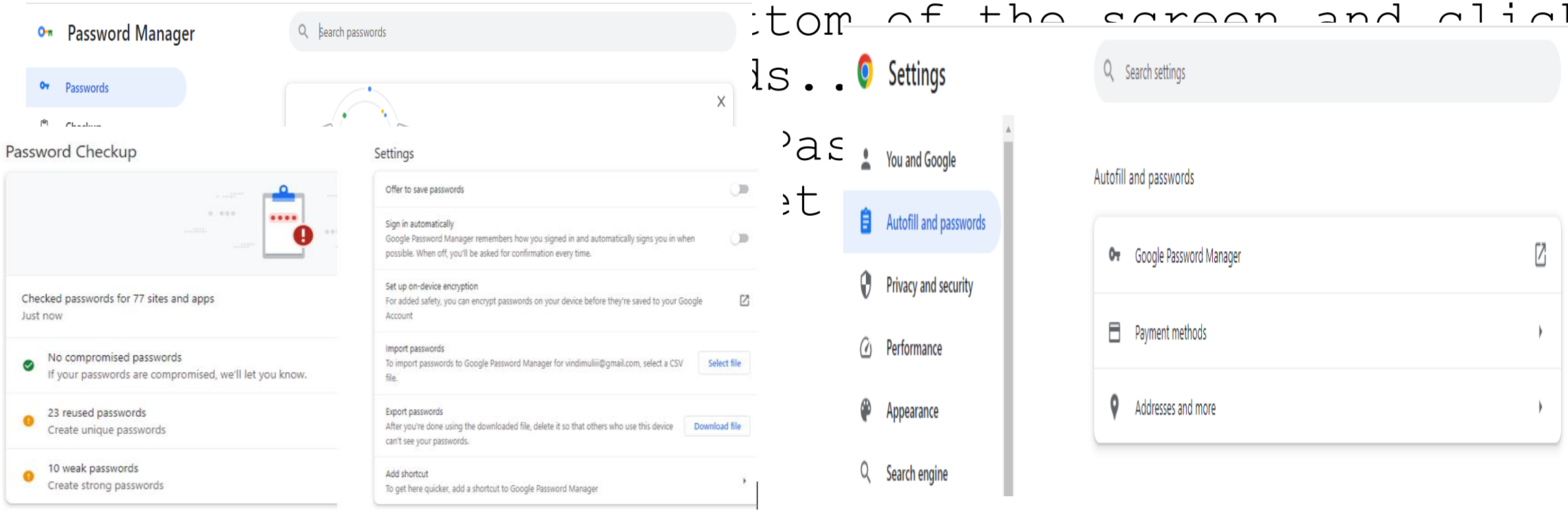
Secure your small home office when working remotely from home by locking the office.

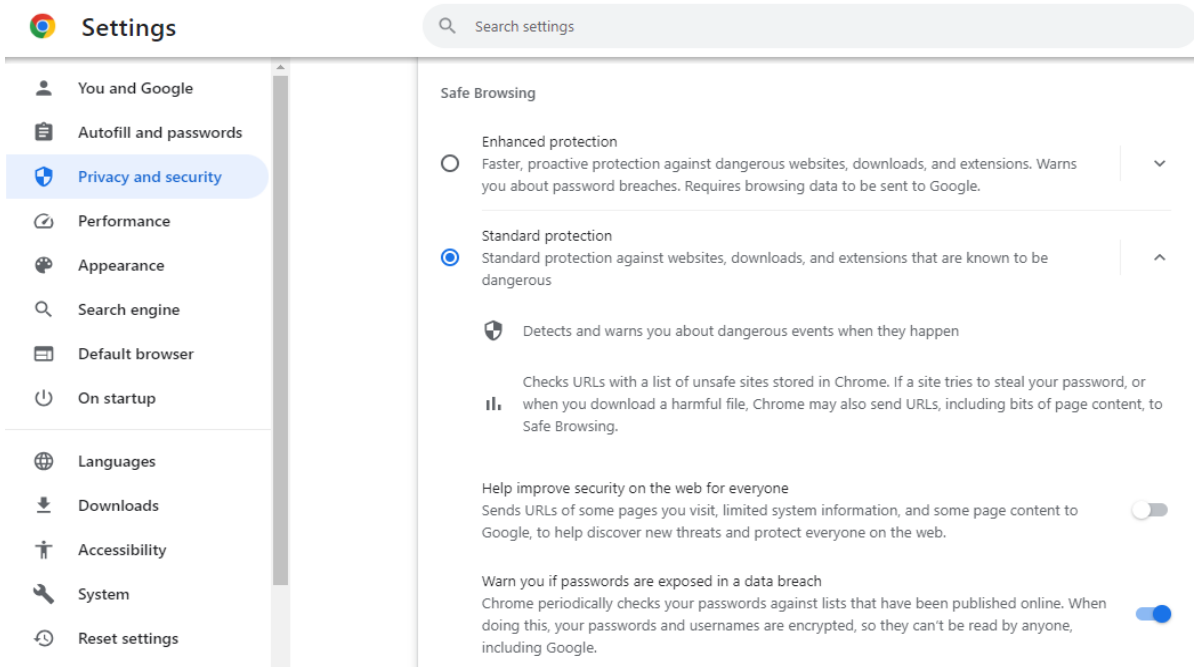
zone areas for work and home devices when working from home to manage and access to sensitive data and files.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Steps to activate remember option in Chrome:

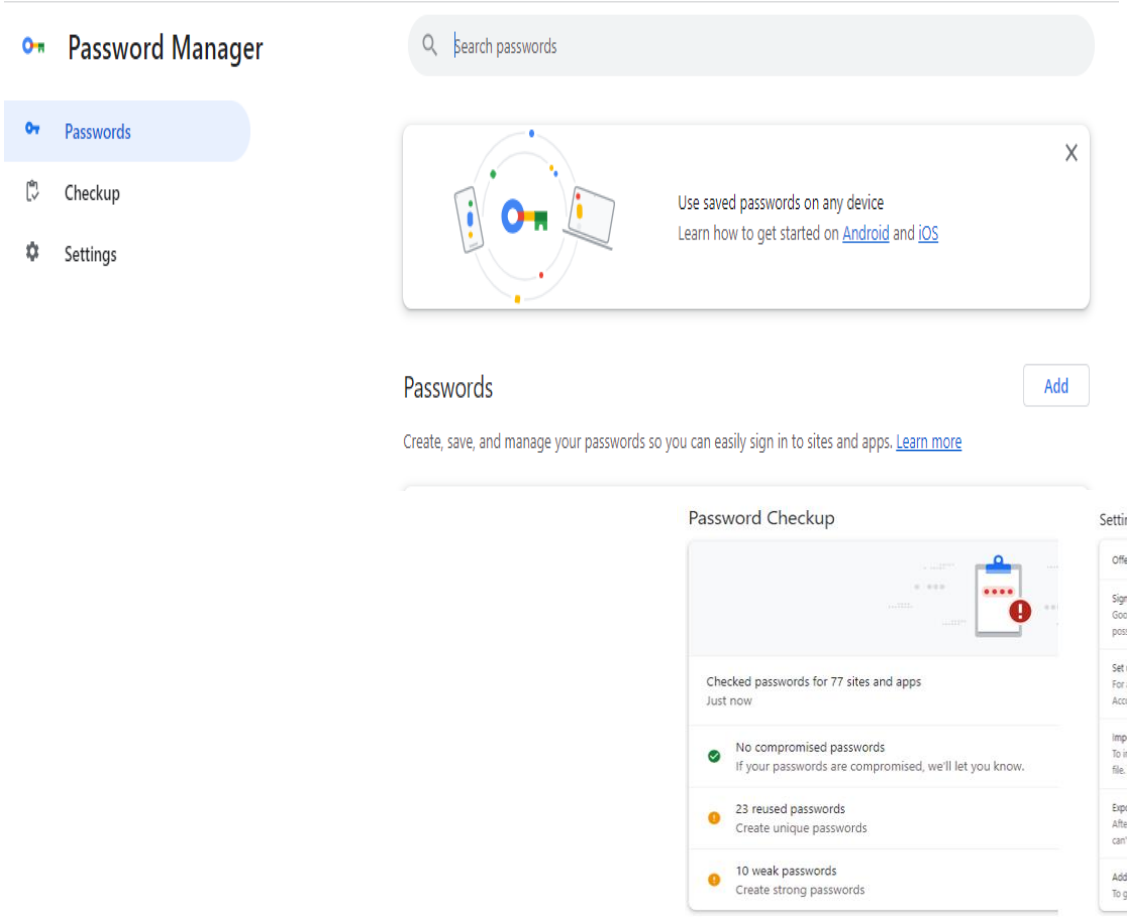
- Open the Google Chrome browser.
- Click the three-bar icon in the top-right corner of the screen > Select "Settings."

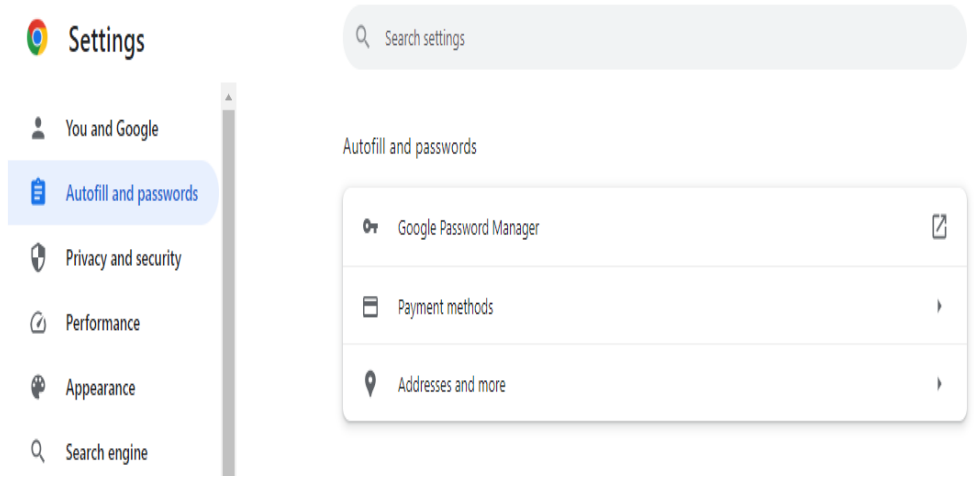




- Activity : automate your security updates
- Steps to automate security updates in chrome
- Open the Google Chrome browser.
- Click the three-bar icon in the top-right corner of the screen > Select "Settings."
- Scroll down to the bottom of the screen and click "Privacy and security settings..."

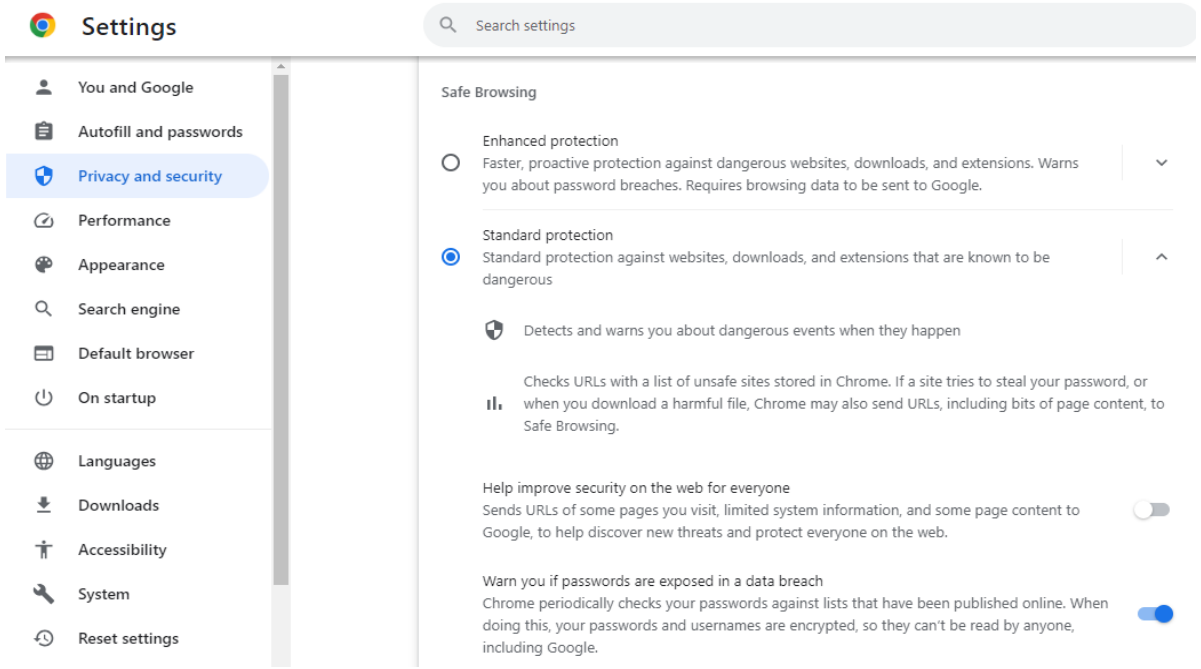
Activity : password checkup





Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Activity : automate your security updates



- Steps to automate security updates in chrome
- Open the Google Chrome browser.
- Click the three-bar icon in the top-right corner of the screen > Select "Settings."
- Scroll down to the bottom of the screen and click "Privacy and Security settings..."

TY CYBER HYGIENE

. 5: CONNECTIVITY CYBER HYGIENE

- 5.0 Learning Outcomes
- Upon completion of this module, the participants will be able to:
  - Introduction to Connectivity
  - Understanding Connectivity
  - Connectivity Cyber Hygiene Practices
  - Online Jobs and Remote Workers
  - Emerging Technology for Connectivity
  - Key Messages Towards Responsible Connectivity

Introduction to Connectivity

- Connectivity refers to the ability of devices, systems, or entities to communicate and share information with each other, often through various forms of networks and technologies.
- In the context of the modern digital age, connectivity is a fundamental concept that underlies our ability to access, exchange, and leverage information, making it a cornerstone of our interconnected world.

Introduction to Connectivity

- Connectivity comes in various forms, each tailored to specific requirements and use cases:
- **Wired Connectivity**: This includes physical connections using cables, such as Ethernet for local area networks (LANs) and fibre-optic cables for high-speed internet.
- **Wireless Connectivity**: Wireless technologies like Wi-Fi, cellular networks (3G, 4G, 5G), and Bluetooth enable devices to connect without physical cables.
- **Satellite Connectivity**: Satellite communication allows global coverage for remote areas and is commonly used for internet access, broadcasting, and navigation.
- **IoT (Internet of Things) Connectivity**: IoT devices connect to the internet through various protocols, such as Wi-Fi, cellular, LPWAN (Low-Power Wide Area Network), or specialized IoT networks.
- **Mesh Networks**: In mesh networks, devices communicate through a decentralized, peer-to-peer model, enhancing redundancy and reliability.

understanding connectivity

Importance of Connectivity

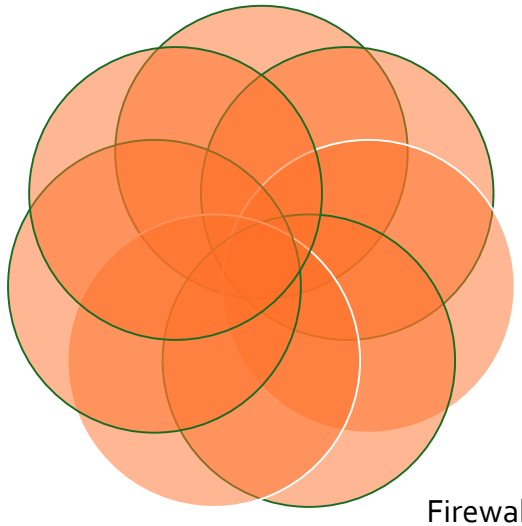
- Information Sharing and communication
- Global Reach
- Economic Growth
- Social Interaction
- Innovation
- Business and Economy
- Social Interaction
- Innovation

.Challenges and Considerations:

- Security
- Reliability
- Data Usage and Bandwidth
- Accessibility

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

5.3 Maintaining the security and privacy of your online activities.



Use Secure and Updated Connections

Password Protection our network an devices

- Regularly update your router's firmware for security patches.

Implement Regular Software Updates

Exercise caution when using public Wi-Fi networks.

Guest Networks for visitors for more security

Add Two-Factor Authentication (2FA & MFA

Firewalls: Enable firewalls on your devices

- Block unauthorized access.
- Be cautious when allowing external access

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

5.3 Maintaining the security and privacy of your online activities.

- Connected Devices change – zone network / (VLAN)
- Log and Audit: monitor / track network activities and detect suspicious behavior(intrusion and unusual behaviors and unknown connections)
- Network Segmentation: Consider segmenting your network for different purposes (e.g., separating IoT devices from your main network). This adds an extra layer of security.
- Secure Hotspots: use a strong password
- Review Device Permissions to apps and devices that connect to your network.
- Limit what info shared
- Secure Network Sharing -share access selectively ; Limit the duration of access to shared resources
- Conduct User Training
- Incident Response Plan: Have a plan in place

Connectivity Cyber Hygiene Practices

- Use Secure and Updated Connections
- Password Protection devices
- Deploy Guest Networks
- Implement Firewalls
- Set 2FA or MFA
- Don t sue open Wi-Fi
- Connect securely via VPN
- Update regularly
- Monitoring Network Activity
- Network Segmentation

- Secure Hotspots with strong authentication
- Review Device Permissions
- Maintain auditing
- User Training for all users on your network
- Backups: Regularly back up your data and network configurations.
- Incident Response Plan: Have a plan in place
- Secure Access Points or disable any unused or unnecessary access points

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Understanding Connectivity

Wired Connectivity

- This involves physical connections
- Uses cables, such as Ethernet cables for local area networks (LANs) and fibre-optic cables for high-speed internet.
- known for their reliability and stability.

Wireless Connectivity

- offers mobility and flexibility.
- Wireless technologies like
  - Wi-Fi
  - cellular networks (3G, 4G, 5G), and
  - Bluetooth enable devices to connect without the need for physical cables.

Satellite Connectivity:

- Relies on orbiting satellites to relay data.
- useful for connectng remote or geographically challenging areas.
- **IoT (Internet of Things) Connectivity**: IoT devices include sensors, smart appliances, and more, connect to the internet using various protocols like Wi-Fi, cellular, LPWAN, or specialized IoT networks.
- **Mesh Networks**: In mesh networks, devices communicate through a decentralized, peer-to-peer model.
- This approach enhances redundancy and reliability because data can take multiple paths to its destination.

Emerging Technology for Connectivity

5G Technology: 5G (fifth-generation)

- wireless technology , faster data transfer speeds, lower latency, and increased network capacity, ideal for applications of IoT, augmented reality (AR), and virtual reality (VR).
- of devices
- For real-time data exchange.

- **Blockchain for Connectivity:**
- Enhance trust and security in connectivity by providing transparent and immutable records of data transactions
- Applicable in securing IoT networks and ensuring the integrity of data exchanged over the internet.

- **Edge Computing**
- processing data closer to the source of data generation,
- reduces latency and enhances real-time c
- For efficient and responsive connectivity,
- essential tech for autonomous vehicles and smart cities.

Mesh Networks:

- Prominent in IoT and connectivity.
- decentralized networks enable devices to communicate with each other directly
- Creates a highly reliable and flexible communication system.

Satellite Internet: Advancements in satellite technology, such as low Earth orbit (LEO) satellite constellations, are improving global connectivity, especially in remote and underserved areas.

5.7 : Emerging Technology for Connectivity

1. Edge Computing: Edge computing involves processing data closer to the source of data generation, which reduces latency and enhances real-time communication.

2. Quantum Internet: Quantum internet is still in the experimental phase, but it has the potential to revolutionize secure communication

3. Quantum Communication Networks:

- These emerging technologies are transforming the way we connect and communicate in an increasingly digital and interconnected world.

4. Terahertz Communication: Terahertz communication involves using terahertz waves for high-frequency data transmission

5. Li-Fi: Li-Fi, or Light Fidelity, uses visible light for data communication.

5.8 Key Messages towards Responsible Connectivity

Satellite Internet: Advancements in satellite technology with improved global connectivity for remote areas

Mesh Networks - prominence in IoT and connectivity and decentralized networks enable devices to communicate with each other directly-highly reliable and flexible communication

Quantum Internet: is still in the experimental phase, but it has the potential to revolutionize secure communication.

5G Satellite Internet:
Combining the power of 5G with satellite technology, companies are exploring ways to offer high-speed, low-latency internet access to even the most remote areas of the world.

Li-Fi: Li-Fi, or Light Fidelity - visible light for data communication transmits extremely high data

Blockchain for Connectivity

- enhance trust and security in connectivity by providing transparent and immutable records of data transactions.
- Applied in securing IoT networks and ensuring integrity of data exchanged over the internet.

Key messages towards responsible use of social media

- Balance Screen Time: Stay healthy
- Community Engagement: Engage positively in online communities
- Secure Access Points: Secure your Wi-Fi networks with strong, unique passwords, and update router firmware regularly to protect against vulnerabilities.
- Continuous Learning: Stay informed
- Responsible Sharing: Be mindful of what you share online.
- Teach Others: Share your knowledge of responsibly
- Incident Reporting: Report incidents appropriately.
- Digital Literacy: Invest in digital literacy education for yourself and others.
- Be a Role Model: Set an example for responsible online behavior.

Key messages towards responsible use of social media

- Promoting responsibly to for the benefits of an interconnected world
- Security and Privacy: Protect your online presence , and privacy
- Critical Thinking: Be discerning when consuming online content.
- Cyber Hygiene: Practice good cyber hygiene .
- Respect for Others: Treat others with respect and kindness online
- Digital Footprint: Be mindful of the digital footprint you leave behind.
- Secure Connections
- Phishing Awareness: Be cautious about clicking on links or downloading files
- Data Management: Understand how your data is being collected, used, and shared
- Online Identity: Be authentic and truthful online.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

6:Email security




Email security measures

Learning Outcomes

Upon completion of this module, the participants will be able to:

1. Recognizing email scams and phishing attempts
2. Email encryption and secure email services
3. Safe email attachment handling
4. Handling suspicious email attachments
5. Email encryption
6. Incident Response and Reporting
7. Steps to take in the event of a cyber-incident
8. Reporting cybercrimes and security breaches
9. Protecting personal information online
10. Safe social sharing and online identity management
11. Dealing with online harassment and cyberstalking

What is Email security ?

Introduction to E-Mail Security

- Email is the most common form of communication in many organisations.
- It is also used to share sensitive information and files as attachments and links.
- Emails are copied to several server across the globe
- Email security vector used by cyber criminals to target and stage a cyber threats and attacks refers to the measures and practices implemented to protect email communications from unauthorized access, data breaches, and malicious misuse.
- Ensuring the security of email communications is essential for safeguarding sensitive information, maintaining privacy, and

Introduction to E-Mail Security

- Email communication is a vector used by cyber criminals to target and stage a cyber threats and attacks refers to the measures and practices implemented to protect email communications from unauthorized access, data breaches, and malicious misuse.
- Ensure the security of email communications is essential for safeguarding sensitive information, maintaining privacy, and preventing unauthorized access to email accounts.

Key aspects of email security issues:

- Emails are susceptible to a range of attacks
- Phishing attack schemes
- Malware attacks - viruses, ransomware, or other forms of malware.
- Spam - Unsolicited, irrelevant, or fraudulent emails that clutter inboxes and may carry threats or scams.
- Data Leaks through various data collection points.

Key aspects of email security

Emails are susceptible to a range of attacks because they are widely deployed

Elements of Email attacks

- Unprotected Backups
- Repudiation
- Fake webpages
- Email Fraud
- Data Leaks
- social engineering attacks
- Business email compromise (BEC)
- Ransomware, Trojan and other malware
- Botnets and DDoS
- Malware attacks - viruses, ransomware, or other forms of malware.

Elements of Email attacks

- Malware attacks - viruses, ransomware, or other forms of malware.
- Spam - Unsolicited, irrelevant, or fraudulent emails that clutter inboxes and may carry threats or scams.
- Data Leaks through various data collection points.
  - Email address Spoofing attacks – phishing
  - Email bombing and Eavesdropping
  - Man in the middle attacks

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Email security and exploitation

The goal of the attackers

- Gain control over an organization (infrastructure /resources)
- Access confidential information
- Exploit to change privileges
- Monitor users' activities
- Perform other malicious actions.
- Disrupt it access to resources.
- Causing serious financial and even intellectual harm.
- Delivers malware for attacks as links and attachments

Email Security Measures

- Use Email Filtering: Enable or use email filtering and spam detection tools provided by your email service provider. These tools can help identify and move suspicious emails to a spam or junk folder.
- Use Antivirus Software on hosts and your network..
- Delete and report any suspicious email
- Implement proper authentication
- Encrypt email communication and attachments
- Connect securely using the secure protocols
  - Transport Layer Security (TLS) is commonly used to secure email transmissions.
- Educate Yourself and team on email security and attacks
  - Recognize phishing attempts and how to handle them
  - How to report any security incidences to follow

Use new generation firewalls and email gateways filter email traffic, block threats, and protect against spam, viruses, and other email-borne threats

Impacts

- Disrupt user productivity
- utilize IT resources excessively
- Distribution mechanism for malware.
- Identity theft result from successful deceptive phishing attacks
- Compromised trusted e-mail systems are often used to deliver spam messages and conduct phishing attacks
- Social engineering - can use e-mail to gather sensitive information
- Entities with malicious intent gain unauthorized access to
- Unintentional acts by authorized users inadvertently send proprietary or other sensitive

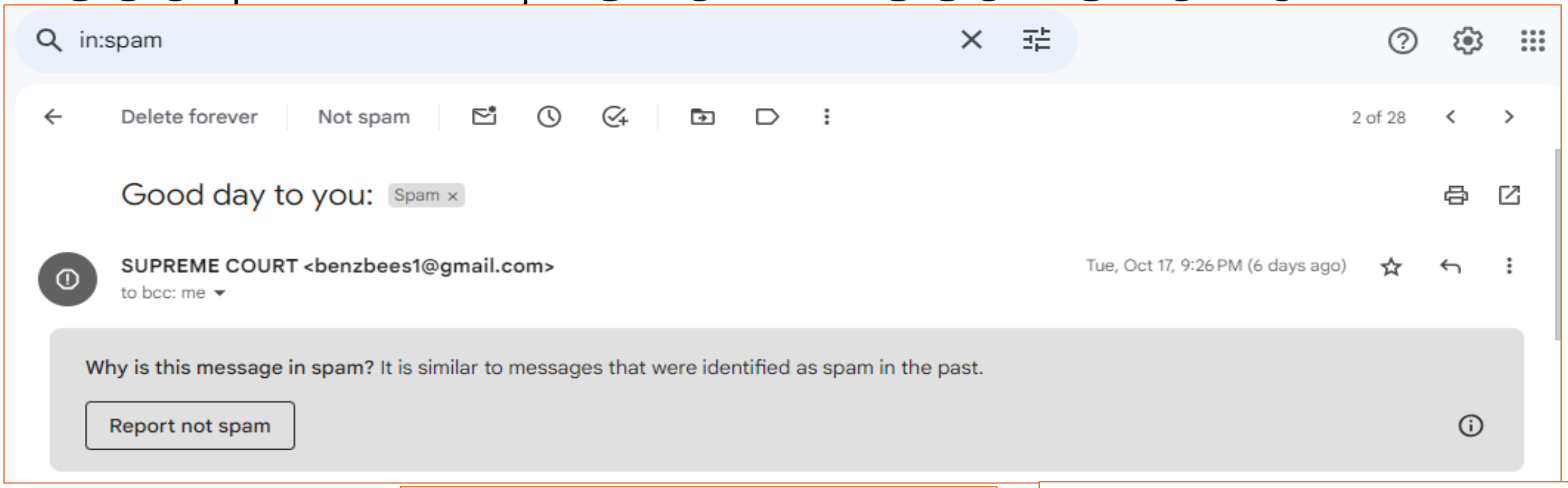
Recognizing email scams and phishing attempts

- Mails are unsolicited, vague, not addressed to the target by name
- Message may have no subject or is a Bcc to recipient
- Pressure to comply in short timeframes and
- requests for secrecy
- Come from unknown sources but purport to be knowing you - those you don't trade with
- Reply back field for ' reply' to address point to a different e-mail address
- Contain attachments/ URL / hyperlink to other sites (hover mouse over it to display the true URL ; don't click it) or type it into the browser to check the expected site.
- This technique is known s known as obfuscation).

- Email refer to current large scale catastrophic news in the subject lines or body.
- Messages contain little other specific or accurate information to build trust
- Contain common mistakes (spelling and grammar, typos or use odd phrases)
- The tone is extremely unfriendly with unrealistic threats and a sense of urgency
- Addresses are spoofed - incorrect versions of the purported organisation / domain
- Contain incorrect or poor versions of an organisation's site
- ask the user to reply to the email, and engage to elicit confidential information.
- Check for Poor Grammar and Spelling

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Recognizing email scams and



SUPREME COURT OF UNITED STATES.
Address: 1 First St NE, Washington, DC 20543, USA.
From: John Glover Roberts Jr, Chief Justice of the Supreme Court of the United States.

Good day to you:

However, due to humanitarian ground and sympathy and because i don't want your payment cancel so i immediately called up a meeting and explain your matter as regards your payment which was resolved that the payment charges of $450 USD will be reduced to $150 USD which it's barest menial in order to enable you afford to pay the fee so that your FUND will be delivery to your home address by Government Authority Diplomatic Agent to make sure that you did not pay any fees again and your delivery Fund Package will not be hold by any power or force again and your delivery will be done within 5hours you send the only fee $150

However, due to humanitarian ground and sympathy and because i don't want your payment cancel so i immediately called up a meeting and explain your matter as regards your payment which was resolved that the payment charges of $450 USD will be reduced to $150 USD which it's barest menial in order to enable you afford to pay the fee so that your FUND will be delivery to your home address by Government Authority Diplomatic Agent to make sure that you did not pay any fees again and your delivery Fund Package will not be hold by any power or force again and your delivery will be done within 5hours you send the only fee $150

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Recognizing email scams and phishing attempts

We want you to know that we are indeed very sorry for any inconveniences any delay this must have caused you in having your fund delivered to you long before now. You will never ever regret paying the fee. This is a promise to you after all your pains in the past as we are here to serve you as our word is our bond to you.

Confirm the receipt of this e-mail by you immediately and be rest assured that you will be smiling at your home once you comply with the above directives now. Your urgent response to this email now will go a long way in helping us ensure your delivery Fund is released to you within five hours of you acting as instructed you now.

Thank you for your understanding. May God bless you and bless the United States of America.

Yours Truly In Service,
Hon.John Glover Roberts Jr
Email:johngloverroberts1@aol.com
Phone:+1(201)897-9884

CHIEF JUSTICE OF THE SUPREME COURT OF UNITED STATES.

Please we want you to know that you have from now till 48hrs to effect the required payment so we can clear, release and effect the delivery of your fund worth US$6.5 Million us dollars in our care to home address, so we advice you to pay the $150 usd. via iTunes Card and send the copy of the $150 usd iTunes to me because i don't want you to lose your Fund.

Send the $150.00 us dollars via iTunes Card, google play or steam wallet and send us the Copy of the card.

After payment has been made kindly send reconfirm to us your correct home address for your 5 hours delivery today.

Your Full Name :.....
Phone Number:.....
Home address:.....
..

Mitigation

- Is Encryption a Requirement? Encrypt
- Configure, Protect, and Analyze Log Files
- process and analyze the log files and review alert notifications.
- Perform Periodic Security Testing
- Periodic security testing of the mail system
- Back up Data Frequently
- back up the mail server on a regular basis to reduce downtime in the event of a mail service outage and support com
- Organizations require malware scanning and spam filtering capabilities at the mail client and the mail system levels. Organizations should also conduct awareness and training activities for users, including telecommuters, so that users are better prepared to recognize malicious mail messages and attachments and handle them appropriately.

Email encryption and secure email services

Here's an overview of email encryption and secure email services:

- Email encryption involves the following
- Converting the content of an email message into a secure, unreadable format (cipher text) that can only be deciphered by authorized recipients.
- It prevents unauthorized access to the content of emails, ensuring the confidentiality and privacy of your communications.
- End-to-End Encryption for email content between sender and receiver
- Secure Email Clients by ensures available encryption methods re supported.
- Management of encryption keys
- User Experience : use user-friendly secure email services
- Secure Email Services and the built-in security features like privacy-focused tools
- Secure communication through the privacy policies that enhance user privacy.
- Open Source Software: Some secure email providers use open-source software to improve transparency and security.
- Anonymous Sign-Up: Some providers allow users to sign up for accounts without revealing personal information, enhancing anonymity.

Safe email attachment handling

- Scan the email with antimalware
- Watch out for dangerous file formats
- Pay careful attention to the sender
- Pause at poor language or odd requests
- Don't open unexpected attachments right away
- Update your system and settings

Handling suspicious email attachment

- Don't open unexpected attachments - opening it will trigger suspicious activities embedded
- Do Not Click on Links or Download Attachments
- Examine the Sender's Email Address
- Scan the file with deep inspection anti malware
- If you have a sandbox upload for scanning
- Verify Unsolicited Requests for personal or financial information, such as passwords, credit card details, or Social Security numbers
- Do not hover Over Links

- Contact the Legitimate Source
- Use Antivirus Software on hosts and your network.
- Delete the Email
- Report any suspicious email
- Change Passwords

- Use Email Filtering: Enable or use email filtering and spam detection tools provided by your email service provider. These tools can help identify and move suspicious emails to a spam or junk folder.

Email encryption and secure email services

- Email encryption involves the following
- Converting the content of an email message into a secure, unreadable format (cipher text) that can only be deciphered by authorized recipients.
- It prevents unauthorized access to the content of emails, ensuring the confidentiality and privacy of your communications.
- End-to-End Encryption for email content between sender and receiver
- Secure Email Clients by ensures available encryption methods re supported.

Management of encryption keys

- User Experience : use user-friendly secure email services
- Secure Email Services and the built-in security features like privacy-focused tools
- Secure communication through the privacy policies that enhance user privacy.
- Open Source Software: Some secure email providers use open-source software to improve transparency and security.
- Anonymous Sign-Up: Some providers allow users to sign up for accounts without revealing personal information, enhancing anonymity.

Maintaining a Secure Mail System

- Configure, Protect, and Analyze Log Files – they record of suspicious behavior on failed and successful intrusions, initiate alert notifications and assist in system recovery and post-event investigations.
- Organizations require both procedures and tools to process and analyze the log files and review alert notifications.
- Back up Data Frequently
- The mail administrator should back up the mail server on a regular basis to reduce downtime in the event of a mail service outage and support compliance with regulations on the backup and archiving of data and information, including those found in e-mail.
- Protect against Malware
- Organizations require malware scanning and spam filtering capabilities at the mail client and the mail system levels. Organizations should also conduct awareness and training activities for users, including telecommuters, so that users are better prepared to recognize malicious mail messages and attachments and handle them appropriately.
- Perform Periodic Security Testing
- Periodic security testing of the mail system confirms that protective measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the operational mail system. Organizations should consider using a combination of techniques, including vulnerability scanning, to assess the mail system and its supporting environment.

Email encryption and secure email services

1. Secure/Multipurpose Internet Mail Extension - S/MIME

This is an encryption tool used with iOS devices and relies on a centralized authority to pick the encryption algorithm. It is also built into web-based email companies such as Gmail and Outlook and android emails.

2. Pretty Good Privacy/Multipurpose Internet Mail Extension - PGP/MIME

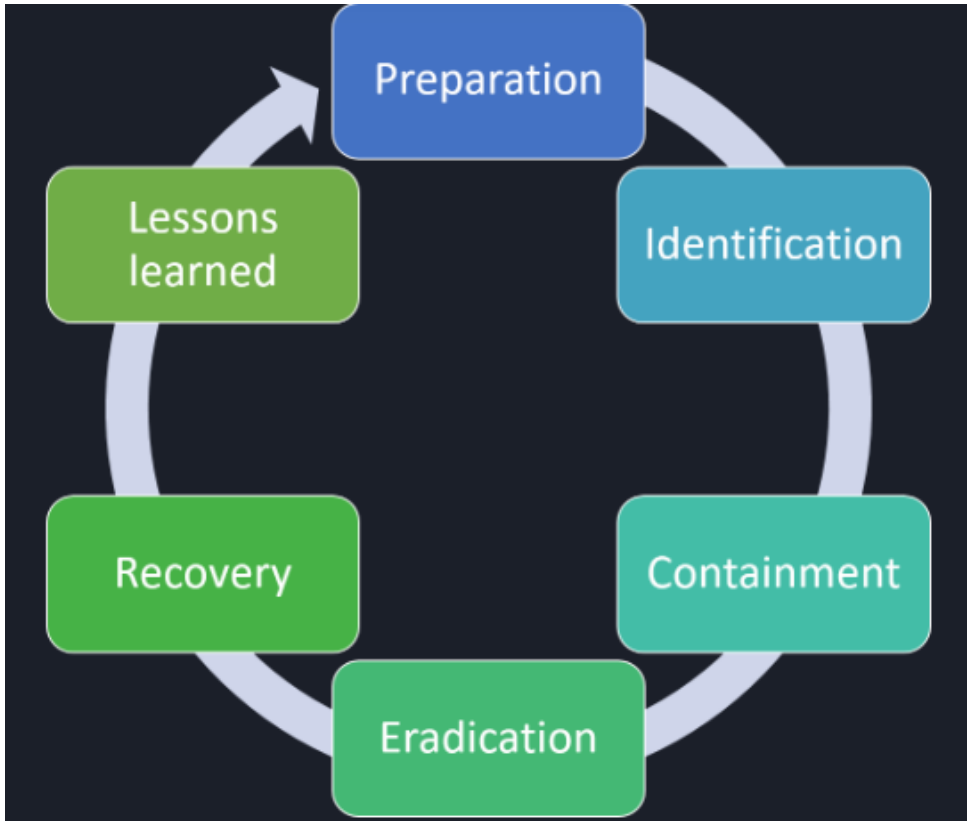
This is another tool that relies on a decentralized trust model and was developed to address security issues facing plain text messages but it requires a third-party encryption tool.

3. PGP/MIME is most common for personal or organizational use and is compatible with Android devices. It can also be used in VPNs, whereas S/MIME cannot

Incident response and reporting

- Incident response refers to the process of identifying, managing, and mitigating security incidents related to email communications.
- Security incidents can encompass a wide range of threats, including
  - phishing emails embedded with malware
  - infected attachments and links and lead to data breaches.
- An incidence response plan helps organizations to effectively address and recover before, during and after an incidents.

Stages in Incidence Response



Incident response and reporting (cont)

Stages in incidence response plan

Step 1. Preparation

This stage includes forming an internal incident response, reviewing your security tools for your network and prioritize known security issues or vulnerabilities and fix them.

Step 2. Identification

The criteria and actions to be followed for assessing a cyber-attack on case it occurs is defined including the information to be collected. The tools to be used for identifying the incident are also defined

Step 3. Containment

The actions to be taken to stop a cyber-attack and extended damage are laid out

Step 4. Eradication

The steps to be taken to contain the threat and restore operations and business continuity are defined in this stage depending with the outcome of the identification stage.

Step 5. Recovery

The purpose of this phase is to bring affected systems back into the production environment, assess the damage and review what went wrong, repair or restore systems back to operations.

Lessons Learned

After any incident follows a debriefing of lessons learned on what went wrong how the incident was handled, what worked and outline the path to improvement.

Steps to take in the event of a cyber-incident

1. **Document ho**w the attack happened,
2. **Mobilize the various** specialists of the cybersecurity Incidence Response team to identify and analyses the scope of the attack.
3. **Identify and** contain the attack by isolating the affected hosts or devices or
4. **Assess t**he extent of the breach - determine what critical resources are compromised and any entry points available for further attacks.
5. **Report the** attack through the right personnel and department.
6. **Document** the lessons learned and the procedures to be initiated to stop future attacks.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Dealing with online harassment and cyberstalking

- Online
- Internet is the new public space
  - We meet people
  - We share opinions / ideologies
  - We obtain information
  - We date and interact
  - We exchange emotions – the good, the bad and the ugly




Cyberstalking

- Cyberstalking is when someone follows you through all you electronic communication, social media, and other technology to instill fear or threaten physical harm.
- It uses the form of social media insights like liking every post from a long time, email, direct messaging, or other electronic means of interaction to harass, scare, or threaten with physical harm.
- come in various forms, such as bullying, sexual harassment, or other unwelcome attention around your life and activities.

Signs of cyberstalking and cyberbullying

- Withdrawal from family and friends activities
- Suffer an unexplained drop in grades.
- Unexplained reluctance to go to school, specific classes, group activities.
- changes in mood, behaviour, sleep, appetite, show signs of depression
- secretive about their cell phone or computer activities.
- sad, angry, or distressed during or after an online activity.
- Appearing anxious when viewing a text, email, or social media post

Impacts

- Higher rates of depression and anxiety
- Reduced feelings of self-worth
- Difficulties sleeping and increased bedwetting
- physical issues such as headaches and stomachaches
- Increased suicide attempts and research shows that cyber bully victims are two to nine times more likely to report suicidal thoughts.
- Increased instances of eating disorders especially among girls.
- Truancy for school going adolescents and youths
- Poor grades in school
- Increased instances of drug and substance abuse

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Dealing with cyberbullies

- Limit your online connection time.
- Never open email messages from sources you do not recognize or from known sources of unwanted communications.
- Blacklist or allow list accounts.
- Change your email address, ISP or phone
- Retaliation will heighten abuse-Ignore!
- Its advisable to consult an attorney on action
- Change your browsing - Change user names and accounts
- Beware of Phishing attempts and dot clink am
- Be cautious of unsolicited emails.
- Avoid clicking on links or downloading
- Verify the legitimacy of email senders
- Secure Your Devices - Ensure your computer, smartphone, and other devices are protected with up-to-date antivirus and security software.
- Avoid Public Wi-Fi and open Wi-Ffi - often less secure.
- Avoid accessing sensitive email accounts when connected to public Wi-Fi.
- Update and Patch Software

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Parental Strategies for Dealing with CyberBullying

Hi Ve JYT e value your privacy.

We will always protect and respect your privacy, while giving you the transparency and control you deserve. Learn about our privacy efforts

Tracking prevention

Websites use trackers to collect info about your browsing. Websites may use this info to improve sites and show you content like personalized ads. Some trackers collect and send your info to sites you haven't visited.

Tracking prevention

Basic

- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

Balanced (Recommended)

- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

Strict

- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Blocked trackers

View the sites that we've blocked from tracking you

Security

Manage security settings for Microsoft Edge

Manage certificates

Manage HTTPS/SSL certificates and settings

Microsoft Defender SmartScreen

Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen

Block potentially unwanted apps

Blocks downloads of low-reputation apps that might cause unexpected behaviors

Website typo protection Are you satisfied with website typo protection?

Warn me if I have mistyped a site address and may be directed to a potentially malicious site.

Use secure DNS to specify how to lookup the network address for websites

By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

- (•) **Use current service provider**
  Your current service provider may not provide secure DNS
- ( ) **Choose a service provider**
  Select a provider from the list or enter a custom provider

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Reporting CyberBullying from the Online Platform





- Visit the National KE-CIRT/CC website https://ke-cirt.go.ke/ and look for 'Report An Incident' option.
- Click on 'Report.'
- In provided spaces, detail your case, including name, organization, contact address, subject (could be abusive content) and an area for a remark.
- Click 'submit' to send your complaint

- NB : Every website has a Report link at the bottom of every page
- Be sure to capture evidence for the case

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

What can we do to protect ? Building resilience

- Bullying programs volunteer to campaigns
- Schools -provide training for teachers around physical, social, and verbal bullying behaviors.
- Implementing conversation bots where students defended the victim and bots supported bullying behaviors
- Anti-bullying intervention programs to reducing bullying behaviors.
- Blocking the user

How to be proactive about cyberbullying

- Ensure that your child only friends and chats with people on social media that they know in real life
- Ensure that privacy settings are set on all your child's social media accounts
- Make sure your child knows not to share or give out passwords
- Ensure that your child knows how to block, delete or report anyone who is upsetting them online
- Advise on screen time best practises

Safe social sharing and online identity management

- Protect your privacy, reputation, and personal information.
  - Limit the amount of personal information visible to the public including :
    - Personally identifying Information:
    - Sensitive information on your daily routine, travel plans, family members.
    - your exact location in real-time
    - full address, phone number, or financial details on public profiles.
  - Use a Pseudonym for greater anonymity
  - Review and Adjust Privacy Settings - regularly review your privacy
  - Report and Block Abusive Users
  - Separate Professional and Personal Profiles

The right to be forgotten

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" if one of a number of conditions applies.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Safe social sharing and online identity management

- Regularly Back Up Data:
  - Use secure cloud storage an strong encryption
  - Regularly back up important data and documents
- Educate Yourself: Understand latest cybersecurity trends / best practices
- use sites with secure websites with "https://" in the URL /address bar.
- Think Before You Post – consider the consequences of your content; once posted, internet will not forget or forgive it!
- Monitor and Manage Tags and Mention
- Be Sceptical of Unsolicited Messages:
- Verify Contacts and Connections before accepting them – Beware of requests from unknown or suspicious accounts

- Avoid saving credit card information on online shopping websites unless it's necessary and trusted.
- Regularly Monitor Financial Statements – Review credit card statements and identify and report unauthorized transactions.
- Consider setting up

Protecting personal information online

- Use Strong, Unique Passwords with a mix of letters, numbers, and special characters.
  - Use a different password for each online account
  - Consider using a reputable password manager to manage passwords.
  - Enable Two-Factor Authentication (2FA) for additional proofing of authentication

Secure Your Devices

- Install a reputable antimalware and lock your devices with a passphrase.
- Review installed applications and permissions
- Uninstall unwanted apps no longer used.
- Change device default passwords before deployment.

Enable Two-Factor Authentication (2FA) for additional proofing of authentication

Beware of Phishing Scams through unknown emails

- Do not click links or download attachments.
- Do not respond with any information.
- Verify the legitimacy of the sender..

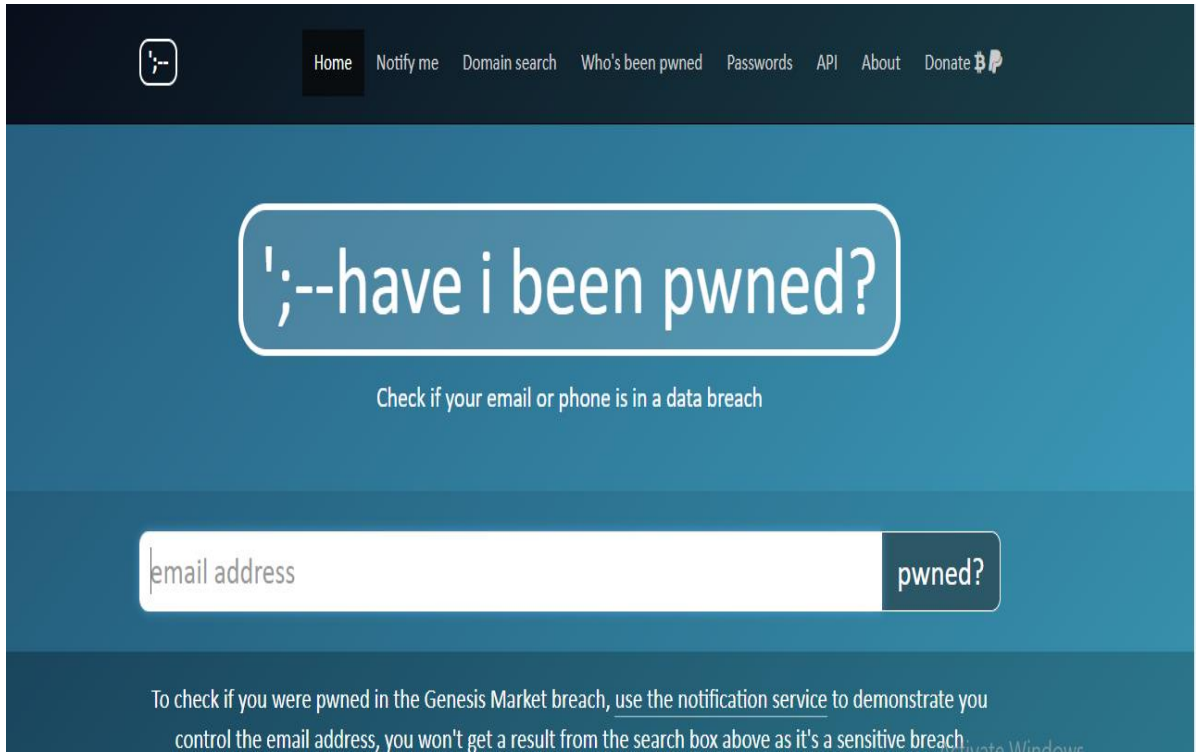
Understand Platform Policies of service and privacy policies

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT technology transforming lives

Check if YOU ARE PWNED

Incase you have been compromised :

- Change passwords
- Ask to log out of all devices
- Understand and review your email security and privacy settings
- Review your app permissions
- Review your digital footprints
- Clean your devices with antimalware



Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

KEEPING MONEY SAFE ONLINE
Introduction to Digital Money?

- Digital money refers to any form of money or payment that exists purely in electronic form. And not the traditional bank notes banknotes.
- Digital money is intangible
- Relies on computer networks and digital storage systems for transactions and record-keeping.
- Exists in various forms of electronic currency : cryptocurrency, mobile money and - prepaid cash and vouchers
- Powered by technologies that power them.
- Its money transitioned from physical cash to digital forms of payment.
- Has a high impact it has on current economy
- There are security and rules which govern them.

Digital money involves recognizing its diverse forms, comprehending the underlying technologies, appreciating its impact on finance, prioritizing security, and being aware of the regulatory landscape.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Digital Money Cyber Hygiene Practices

- These refers to the behaviors one should conform to ensure safety while transactions committed online are secure and private and protected.

1. Use Secure Networks: connect via secure protocols and trusted Wi-Fi networks, especially when making financial transactions. Avoid public Wi-Fi for sensitive activities.

2. Update Software Regularly: Keep operating systems, apps, and antivirus programs up-to-date. Updates often include security patches that protect against the latest threats

3. Enable Two-Factor Authentication (2FA): Enable 2FA wherever possible. This adds an extra layer of security by requiring a second form of verification in addition to your password.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Emerging Technologies in finance and money

- These refers to the new solutions which are coming up to cover the gap which exists in the financial field. They are meant to improve efficiency, security and also aid in accessibility of money management.

1. Blockchain

- A cloud-based contactless banking architecture significantly convenient and less prone to errors.
- uses bitcoin technology - cryptocurrency.
- BC Tech is safe and dependable - protects data, verify and identity, record transactions, sign contracts, and improve traceability.
- Ideal Cloud banking solution for smooth global payments, .

2. Embedded Finance

- a new tech in financial services that improve client loyalty
- Facilitates speedy transaction with a few clicks on a store's website
- allows non-financial platforms to integrate payments for loans, insurance, debit cards, and investment instruments.
- beneficial for e-commerce enterprises

3. Big Data

- Provides huge amounts of organized and unstructured data that financial institutions use to forecast consumer behaviour and build strategies.
- analyses and generates massive volumes of data held internally within a corporation to give essential facts for timely decision-making. every second.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Emerging Technologies in

Open Banking

program allows banks to exchange data on their customers with fintech startups and other financial institutions via programming interfaces (APIs), which enable a website or app to access the bank's database.

Regtech

- enables financial institutions to monitor the correctness and legality of their actions automatically without the need for non compliance to fintech legislation
- No need for lawyers to oversee process or face fines for non compliance
- Identifying clients, processing and preserving data,
- Calculates financial risks
- Assists in adhering to legal requirements and avoiding fines.

Robotic Process Automation (RPA)

- utomate back-end office activities to finish work more quickly, save money, and boost organizational efficiencies
- Enables employees to focus on more critical tasks like customer services such as customer onboarding, security checks, credit card and mortgage processing, etc.
- .

Artificial Intelligence (AI) and Machine Learning (ML)

- Allowed banks to handle massive amounts of data
- Provides ability to evaluate real-time trends
- aid in speedy decision-making.
- has decreased the time and cost of several banking processes

Neo Banks

- Are digital banks convenient and accessible, less expensive - no physical branches.

transactions will be conducted online, bank branches will continue to play a minor role

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Key Messages for Keeping Money Safe

- **Monitor Accounts Regularly:**
- Regularly check bank and other financial credit card
- digital wallet statements
- Report suspicious activity immediately.
- Set up account notifications and
- report any unauthorized transactions promptly.

- . **Be Cautious Online:**
- Be wary of clicking on suspicious links, downloading unknown attachments, or responding to unexpected emails or messages.
- Verify the authenticity of emails messages.
- Avoid interacting with unsolicited communications

- **Use Reputable Services:**
- Rely on well-known financial services.
- Use official apps and websites for transactions.
- Download apps from official app stores
- verify legitimacy of online services before providing any financial information.

- **Protect Personal Informa*tion:***
- . Avoid sharing sensitive details online or over the phone .
- verify the identity of individuals or organizations requesting personal data.
- **Stay Informed** on common scams and fraud tactics.

- **Use Secure device and network**
- Protect your devices with passwords, PINs, or biometric features.
- Use secure, password-protected Wi-Fi networks for online transactions.
- Regularly update passwords, secure your devices with lock screens, and

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

Safe Online shopping and Banking & shopping

- This refers to the tricks to ensure one is safe while shopping online and transacting online without getting scammed or losing personal information to cybercrime.
- Online banking is the method by which people transact online without having to visit the banks.
- very convenient method but very risky if one does not keep safe online.
- Safe banking ensures one is aware of the tricks used by cyber criminals to steal personal information.

- **Protecting your financial Info Online**
- Always use unique and secure and strong passwords for your mobile banking and wallets.
- Avoid using personal bio data and other easy passwords to guess .
- Avoid public wifi when shopping or transacting online
- Avoid giving out your personal information like card number.
- Shop or transact with verified financial services only - avoid falling to traps of the many cons available online nowadays.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Safe Online Shopping and Banking:

- **Use Strong, Unique Passwords and enable Two-Factor Authentication (2FA**
- **Secure Your Devices:**
- Keep your devices (computers, smartphones, tablets) up-to-date with the latest security patches and updates.
- Use strong device passwords, PINs, or biometric authentication methods (e.g., fingerprint or facial recognition).
- Install reputable antivirus and anti-malware software to protect against malware and viruses.
- **Use Secure and Up-to-Date Wallets:**
- If you're using a cryptocurrency wallet, ensure that it's from a trusted source and always use the latest version.
- Use hardware wallets or other secure cold storage methods for significant cryptocurrency holdings.
- **Beware of Phishing Scams**
- Verify the legitimacy of the sender
- Be especially vigilant with emails or messages that contain urgent requests or suspicious links.
- **Only Use Reputable Exchanges and Services:**
- If you use digital money exchanges, make sure they are well-established, regulated (if applicable), and have a track record of security.
- **Regularly Monitor Your Accounts:**
- Frequently check your digital money accounts and transactions for any unauthorized or suspicious activities.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Secure online shopping websites

- There are several online website which one can shop online.

  Below is an example of them:

  = Jumia

  = Amazon
  = Aliexpress
  = Alibaba

  = Flipkart

  = Kilimall

  = Glovo

- **Safe Online Shopping and Banking**
- Recognizing secure online shopping websites
- Protecting your financial information during online transactions
- Banking and payment app security

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Securing Access to Devices and Services

- Introduction
- Understanding Access Control and User Authentication
- Cyber Hygiene Practices for Access Control and User Authentication
- Accessing e-Government Services
- Emerging Technology for Access Control

Cyber Hygiene for Social Media and Messaging

- Understanding Social Media and Messaging
- Cyber Hygiene Practices for Social Media, Messaging and Internet Use
- Child Online Protection Practices and Resources
- Emerging Technology in Social Media
- Key Messages towards Responsible use of Social Media

Cyber Hygiene for Social Media and Messaging

- Respect Privacy of others - Do not share or post content without getting appropriate permission.
- Think Before You Post – review the consequences of potential consequences
- Be Kind and Respectful - Avoid engaging in cyberbullying, hate speech, or harassment.
- Protect Your Personal Information
- Understand Privacy Settings: Familiarize yourself with the privacy settings
- Adjust settings to control who can see your content and information.
- Critical Thinking: Apply critical thinking when consuming content. or read online is accurate, so question and verify information.
- Online Etiquette: Follow proper online etiquette. Remember that your comments and posts can have a significant impact on others.
- Digital Footprint: Be aware that your online actions contribute to your digital footprint. Future employers and educational

Guidance for People Living with Disabilities

- How does a genuine person or organization reach out to you?
- How to identify suspicious messages or calls.
- What to do when you suspect or recognise a social engineering scheme.




How doe a genuine person conduct you ?

- 1. verified accounts – email / social media
- Phone call with matching identity
- Chats and followed by calls
- Text message followed by calls – needs verification
- physical identity

How to identify suspicious messages or calls

- Step 1: The message is irrelevant to you.
- Step 2: The text message contains misspellings or poor grammar.
- bad grammar scam text
- Step 3: Abnormally long numbers.
- The message is from purpoted a bank or other financial institution.
- Beware of abnormal-looking numbers that claim to be banks
- Step 4: It offers random prizes.
- Step 5: The text message contains a suspicious link.
- Step 6: The message's tone is urgent or requests your immediate action.
- Step 7: The text offers a fake refund.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT

How to identify suspicious messages

- Congratulations, You've Won when you did not subscribe
- Asks you to Verify or Update Your Account
- Warns about Account alert scam text
- Assist an Acquaintance or Family Member
- Got a weird message claiming to be from someone you know and asking you to buy gift cards? This is another common scam you should never fall for.
- Pretend it is your CEO scam text
- Received a package – needs address to deliver
- Two-Factor Authentication reset




How to identify suspicious calls

- They call at odd hours
- They disconnect immediately
- They carry Arrest Threats
- Offer you Unwarranted Technical Support
- Fake Charities
- Contest Wins
- scammer
- Debt Relief redress
- People in Danger
- Ask you to share details and codes sent to youth

- Do not respond with details
- Disconnect
- Inform your bank immediately.
- Report any incidents of scam calls,
- Don't Switch off the device – it could be a SIM swap
- Change any passwords on a different device

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development Partnership | Progress | Prosperity | ACWICT

Guidance for People Living with Disabilities

- People living with disability undergo aa lot of cyber- harrassment but very few come out to report for the fear of victimisation despite the evidences existing. The nature of their disability is always an obstacle in getting support coupled with lack of lack of expertise and training in supportive channels of communication.

What are the attributes of good key messages to PwDs?

- Given existing challenges, everyone should strive to
- Simple easy-to-understand language; avoid jargon and acronyms when communicating with PwDs
- Design meaningful information to stimulate action.
- Use active voice to communicate to them - not passive; do not use advertising slogans.
- Tailor and communicate effectively with different target audiences by adapting language and depth of information.
- Outline what you need to communicate relevantly
- Memorable: Ensure that messages are easy to recall and repeat; avoid long, run-on sentences.

Ministry of Information, Communications & The Digital Economy | ICT Authority | UK International Development — Partnership | Progress | Prosperity | ACWICT


HARAMBEE
REPUBLIC OF KENYA


ICT
Authority


UK International
Development
Partnership | Progress | Prosperity


KICTANet
The Power of Communities


ACWICT
technology transforming lives


KILIMO HAKIKA
PRECISION AGRICULTURE


Otermans
Institute


BUSIA
COUNTY
UNITED FOR DEVELOPMENT

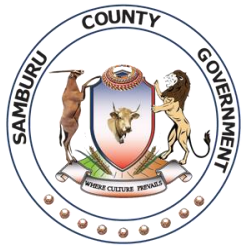

COUNTY OF CHAMPIONS


THE COUNTY GOVERNMENT OF GARISSA
KENYA


ISIOLO COUNTY GOVERNMENT


UMOJA NA UCHUMI
MANDERA COUNTY GOVERNMENT


COUNTY GOVERNMENT OF MARSABIT
THE CRADLE OF MANKIND


COUNTY
SAMBURU
GOVERNMENT


COUNTY GOVERNMENT OF SIAYA


COUNTY GOVERNMENT
OF TANA RIVER
THE LAND OF TREASURE


TURKANA COUNTY
GOVERNMENT
PAMOJA TUJIJENGE


COUNTY GOVERNMENT OF WAJIR
UNITY AND JUSTICE


USAID
SGR WEST
Inclusive Digital Futures Project
DRIVING GROWTH AND RESILIENCE THROUGH DIGITAL EMPLOYABILITY FOR THE YOUTH, WOMEN, AND PERSONS WITH DISABILITIES

THANK YOU

Thank you


Ministry of Information, Communications & The Digital Economy
ICT Authority
UK International Development
Partnership | Progress | Prosperity
ACWICT