UKaid
from the British people

DigiGirls

Keeping Your Smartphones, Tablets and Computers Safe

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

Data Protection

Secure settings for your computer and mobile devices

Device Security

Safe software download and installation

Secure Remote Working

An initiative of
cybersafe.
FOUNDATION

Data Protection

Data Protection

Data protection is the process of safeguarding important information from corruption, compromise or loss.

Data protection is a set of strategies and processes you can use to secure the privacy, availability, and integrity of your data. It is sometimes also called data security or information privacy.

CASE STUDY

https://nation.africa/kenya/business/mobile-lenders-ditch-debt-collectors-to-escape-sting-of-debt-shaming-law-4096420

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Secure settings for your computer and mobile devices

An initiative of
cybersafe.
FOUNDATION

Tip 1: Switch on password protection

Devices such as mobile phones, computers and tablets are commonly used for work to send and receive business emails and sharing of sensitive information which makes these devices a target by hackers trying to steal the information for their personal gain.

- By enabling password protection on your device this will prevent unauthorized users from gaining access to your device and ensure your data remain protected.
- It does not stop at just enabling password protection, it is important to practice a good password hygiene by applying the following:
- Use of Password Manager
- Use a Strong Password
- Enable Two-Factor Authentication (2FA)
- Make Use of Unique Password

Tip 2: Keep your Device up to date

The best ways to protect your device is to ensure it is running the latest update by following these steps:

- Frequently run scans on all your devices to discover missing updates.
- Frequently apply update on your device.

Tip 3: Make sure lost or stolen devices can be tracked, locked or wiped

It is important to enable Mobile Device Management (MDM) on your devices to allow you manage your device remotely in an event it is lost or stolen you can easily track, lock or wipe your data on the device. This removes the risk of your data falling into the wrong hands and the damaging effect it can have on your business.

Tip 4: Install a licensed antivirus

The foundation to having a good security posture is to install antivirus on your device. It is important to have a licensed and properly configured antivirus in your, device to protect you from attacks by bad actors.

Tip 5: Keep apps and software up to date

Vulnerabilities are discovered daily on applications and these vulnerabilities can be exploited by attackers to gain access to your device and steal sensitive information or go to the extreme of damaging your device. Frequently check for software update and apply on your applications to ensure you are protected from zero-day attacks.

Tip 6: Avoid public Wi-Fi hotspot

Using a public Wi-Fi makes you an easy pre for an attacker as they can easily gain access to your device and steal your data. They could also plant a monitoring tool on the network to spy on your internet browsing activities. Unlike a private Wi-Fi most public ones don’t have any form of security in place to protect the users connected to the network.

Tip 7: Leverage built-in Encryption

Encryption helps you protect the data on your disk by converting it into an unreadable format and only becomes readable when the correct password is provided on the encryption software. In the event your device is lost or stolen, the data on the disk cannot be viewed in its readable form.

You can leverage on Microsoft Windows inbuilt encryption “BitLocker” and Apple Mac inbuilt encryption “FileVault” to encrypt your laptop disk.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Device Security

An initiative of
cybersafe.
FOUNDATION

Controlling Access to Data

Access control governs the resources that an unauthenticated user is able to read, modify, or write. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

Access control is a selective restriction of access to data, it consists of two main components:

- **Authentication** is a technique used to verify that someone is who they claim to be. Authentication isn't sufficient by itself to protect data; data protection needs an additional layer.
- **Authorization** determines whether a user should be allowed to access the data or make the transaction they are attempting.

Keeping Your Devices Safe

1. Always use a password
2. Use password manager. Don’t write your password on a piece of paper or store on a notepad on your system to prevent it from falling into the wrong hands.
3. Use a strong password. Your password must contain upper case and lower case alphabets, numbers, special characters and much be at least 8 characters long.
4. Use 2factor authentication
5. Use a different password for different accounts
6. Install a licensed antivirus software
7. Keep apps and software up to date

Keeping Your Devices Safe

8. Keep your device up to date. Ensure it is running on the latest updates
    - Frequently run scans on all your devices to discover the missing updates and apply them
    - Subscribe to vendor’s security awareness channel to get news updates on newly discovered innovative and software updates
9. Make sure lost or stolen devices can be tracked, locked or wiped. Enable mobile device management on your devices to allow you manage your device remotely.
10. Avoid public Wi-Fi hotspot
11. Leverage built in encryption (e.g., bitlocker and Apple filevault

Device Security Strategies

- Secure Wi-Fi Networks
- Strong Passwords
- Deploy Software Solutions
- Wipe Device
- User Access Rights Management
- Data Backup
- Leverage Biometrics

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Safe Software Download and Installation

An initiative of
cybersafe.
FOUNDATION

Safe Software Download and Installation

Tip 1: Avoid Unsolicited Links

The most effective and easiest thing you can do to avoid malware and adware is to avoid downloading any software program or app from an unsolicited link. Avoid downloading anything that you've received a link to via an email, text, or some other personal message unless you completely trust the source.

Safe Software Download and Installation

Tip 4: Free Downloads ≠ Free Software

Free download does not mean that the software is free to use. Before downloading something that is labelled "free" or as a "free download," check to see that the program description clearly states that it's freeware or completely free to use.

Tip 5: Avoid Tricky 'Download' Ads

Don't be tricked by "Download" advertisements. These sorts of advertisements run frequently on software download pages, appearing as giant download buttons. These download advertisements usually go to a malware-ridden page where you get to download something else. Not all software download pages have download buttons either, many are just links.

Safe Software Download and Installation

Tip 6: Avoid Installers and Download Managers

One way these download sites make their money is by wrapping the downloads they serve inside of a program called an **installer** or a **download manager**.

These programs are often referred to users as **PUPs** – Potentially Unwanted Programs; these programs have nothing to do with the program you're trying to download and install.

Tip 7: Choose 'Custom Installation'

During downloads, when choose **Custom Installation** when given the option. This option makes the install process a bit longer with the few extra screens it adds, but it's almost always where the "don't install this" options are hidden. One way to avoid installation-based problems is to choose portable software instead of installable software.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Secure Remote Working

An initiative of
cybersafe.
FOUNDATION

Best Practices for Working Remotely

- Use antivirus and internet security software at home.
- Secure your home Wi-Fi.
- Make sure your passwords are strong and secure.
- Keep family members away from work devices.
- Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.
- Be wary of email scams and your email security.

UKaid
from the British people

DigiGirls

Best Practices for Working Remotely

- Keep work data on work computers.
- Run software updates regularly.
- Use a VPN.
- Encrypt sensitive data in emails and on your device.
- Never leave your bag, briefcase or laptop unattended.
- Don’t use random thumb drives.

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Browsing the Internet Securely

1. Keep your browser and any plugins updated
2. Use a browser that allows you to take your bookmarks with you in between devices
3. Block Pop-ups
4. Use an ad blocker
5. Use a VPN
6. Use a password manager
7. Ensure you have an up-to-date antivirus and firewall protection
8. Beware of public (unprotected) Wi-Fi
9. Https

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION