UKaid
from the British people

DigiGirls

Keeping Your Online Accounts Secure

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Content

- Case Study
- Tips to Protect your Social Media and other Online Accounts
- Safe Web Browsing and Best Practices
- Using Passwords to Protect your Data
- Turning on Extra Security

An initiative of
cybersafe.
FOUNDATION

Case Study

https://techcrunch.com/2017/12/22/that-time-i-got-locked-out-of-my-google-account-for-a-month/

Case Study

https://www.cbsnews.com/boston/news/scammers-hack-facebook-accounts-fake-taylor-swift-tickets/

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Tips to Protect your Social Media and Other Online Accounts

An initiative of
cybersafe.
FOUNDATION

Keeping Social Media Accounts Secure

1. Choose a strong password
2. Use a different password for each social media account.
3. Seal it off by adding an extra layer of security with 2factor authentication.
4. Never click on links without ensuring they are safe.
5. Make sure you scan all attachments for viruses before you download them.
6. Limit the amount of information you share online
7. Review privacy settings

Safe Web Browsing

What does the padlock at the top of your browser window really mean?

What websites shouldn't you be visiting?

Safe Web Browsing

- Do not leave your device unattended to, if you must, ensure to lock the screen.
- Change your password if you think someone may have learned (seen, heard) it
- Observe a clean desk policy
- Do not share personal or sensitive information on social media
- Be wary of links and attachments in emails

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Using Passwords to Protect your Data

An initiative of
cybersafe.
FOUNDATION

What is a Password?

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application, or website.

Passwords can vary in length and can contain letters, numbers, and special characters.

Creating A Strong Password

Passwords are gatekeepers to your most important information. Cyber attackers are opportunistic and can easily crack weak password.

Strong passwords are passwords no one can ever guess; not even your loved ones.

A strong password must meet the following criteria:

- Must contain a minimum of one uppercase letter e.g A-Z
- Must contain a minimum of one lowercase letter e.g a-z
- Must contain a digit e.g 0-9
- Must be at least 12-characters long e.g Abcd1234
- Must contain special characters e.g. ~!@#$%^&*()_-+=

An initiative of cybersafe. FOUNDATION

Creating A Strong Password

A Strong Password **should not**:

- Spell a word or series of words (that make sense together) that can be found in a dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.
- Be a word you use a lot, your favourite colour, your date of birth, pet names, numbers in sequential order, repeated character or series of characters etc. Common offenders include "123456," "password," “AAAA,” and "qwerty".

Topic Activity

Create a strong password

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Techniques For Creating A Memorable Password

An initiative of
cybersafe.
FOUNDATION

Techniques For Creating A Memorable Password

Passphrase Method

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but it is generally longer for added security.

For example, you might choose the easily memorable phrase, ‘Osapa London at Lekki phase 1’ and make your passphrase ‘osapaLONDON@lekkiphase1’

Techniques For Creating A Memorable Password

Storytelling method

In this method you make a sentence out of something that has happened in your life and string the first alphabets of each word to form a password.

A perfect example is a sentence like “The first time I took a French quiz I scored 99% and won a cash gift of 20 dollars.” So, your password will become this **TftItaFqIs99%awacgo20$**.

This password has 22 characters, is a mixture of numbers, symbols, uppercase and lowercase letters.

Topic Activity

Create a password using storytelling method

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password Hygiene Best Practices

An initiative of
cybersafe.
FOUNDATION

Password Hygiene Best Practices

1. Choose a strong password. Choosing strong passwords are critical as they prevent unauthorized access to your physical devices and online account.
2. Avoid Personal identifiers
3. Change all default passwords
4. Avoid using browsers to create and manage passwords.
5. Where possible ensure it is not a dictionary word.
6. Ensure it is unique per platform.
7. Use a password manager. Some popular password managers include, one password, lastpass, dashlane, sticky passwords etc.
8. Turn on an extra layer of security.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password Manager

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Password Manager

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database.

Importance of Password Managers

1. Password managers protect you by helping you create strong, unique passwords for every service you use, and removing your need to enter those passwords.
2. Remember Only One Password
3. Password managers can prevent password-reuse attacks.
4. Password managers can prevent impostor websites from “phishing” you.
5. Password managers track which services you have accounts with, helping you identify unused accounts that you may want to close or delete data from to reduce your online exposure.

Importance of Password Managers

6. Most password managers have password generators that help generate strong passwords.
7. You can still use the form autofill feature when you have a password safe. Instead of letting your web browser save your form information, entrust your password manager to store your personal information safely.
8. You can share passwords to joint accounts with family or coworkers. It is generally not recommended you give away your personal passwords, but for shared accounts, a password manager gives you the option to control who has access to passwords.

UKaid
from the British people

DigiGirls

Topic Activity

Download and setup a password manager

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Extra Layer of Security

An initiative of
cybersafe.
FOUNDATION

Extra Layer of Security

Thumbprint

Eye Sanner

Token

Facial Recognition

Voice Recognition

OTP

An initiative of cybersafe. FOUNDATION

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION