lsp

THEME OF THE MONTH

JUNE 2023

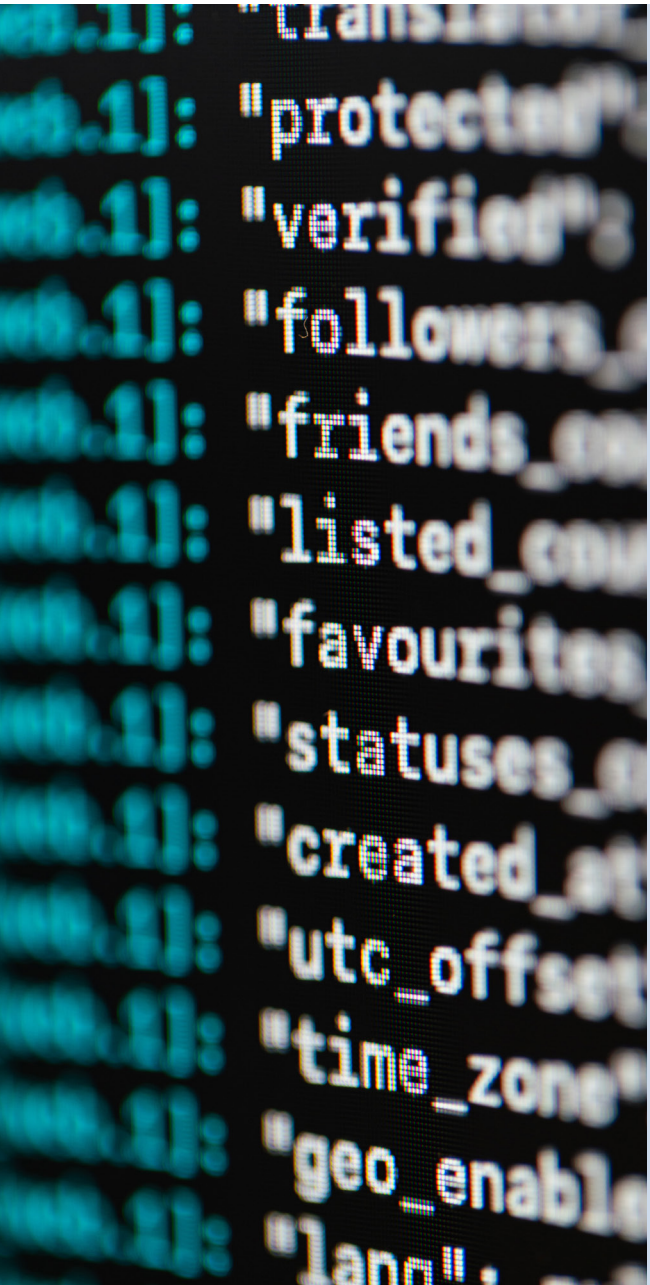
PROTECTING YOUR DIGITAL WORLD: PASSWORDS

Introduction

In this booklet, you will learn how to create and maintain strong passwords to safeguard your online accounts from unauthorised access. With the increasing importance of digital security, understanding password best practices is crucial in protecting your personal and sensitive information.

Why are passwords important?

Passwords serve as the first line of defence for your online accounts. They help protect your personal data, financial information, and digital identity from hackers and cybercriminals. Using strong passwords is essential to minimize the risk of unauthorized access, identity theft, and data breaches.



What is cyber security?

Cyber security refers to the practice of protecting computers, servers, networks, and digital systems from unauthorised access, damage, theft, or disruption of information. It involves implementing measures to prevent, detect, and respond to various cyber threats, including hackers, malware, viruses, ransomware, and other malicious activities.

The primary goal of cyber security is to maintain the confidentiality, integrity, and availability of digital assets, ensuring that data and systems are protected against unauthorised access, alteration, or destruction. It encompasses a range of practices, technologies, and policies designed to safeguard information and mitigate the risks associated with operating in a connected digital environment.

Key aspects of cyber security

Network Security

Protecting networks from unauthorised access, malware, and other threats. This includes implementing firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs).

Application Security

Ensuring the security of software applications to prevent vulnerabilities that could be exploited by attackers. This includes secure coding practices, regular updates and patches, and application security testing.

Data Protection

Safeguarding sensitive data through encryption, access controls, and secure data storage and transmission. Data protection also includes data backup and recovery measures to ensure business continuity in the event of a breach or data loss.

Identity and Access Management (IAM)

Managing user identities and controlling access to systems and resources. This involves implementing strong authentication mechanisms, role-based access controls, and user account management practices.

Incident Response

Establishing procedures and protocols to respond to and mitigate the impact of security incidents. This includes incident detection, containment, eradication, and recovery measures.

Cyber security is an ongoing and evolving field as new threats and vulnerabilities emerge. It requires a proactive and multi-layered approach, combining technological solutions, robust policies, regular monitoring, and continuous education to protect digital assets and ensure the safety and privacy of individuals and organisations in the digital age.

Creating strong passwords

Creating strong passwords is crucial to protect your online accounts and personal information. Here are some tips to help you create strong passwords:

Length

Aim for a minimum of 12 characters or more. Longer passwords are generally more secure.

Complexity

Include a combination of uppercase and lowercase letters, numbers, and special characters (such as @, $, *, etc.). This increases the complexity and makes the password harder to guess.

Avoid personal information

Do not use easily guessable information like your name, birthdate, or pet's name. Hackers can easily obtain this information from public sources.

Avoid common words

Avoid using common words or dictionary terms, as they are easy for hackers to crack. Instead, consider using a combination of unrelated words or use a passphrase.

Passphrases

Consider using a passphrase instead of a single word. A passphrase is a longer sequence of words that are easy for you to remember but difficult for others to guess.

Unique passwords

Use a unique password for each of your online accounts. This way, if one account is compromised, the others will remain secure.

Avoid patterns or sequential characters

Avoid using patterns like “123456” or sequential characters like “qwerty” as they are easily guessable. Mix up your characters and avoid predictable patterns.

Avoid common passwords

Stay away from commonly used passwords like “password,” “123456789,” or “admin.” These passwords are frequently targeted by hackers.

Password managers

Consider using a password manager tool to generate and securely store your passwords. Password managers can help you create strong, unique passwords for each site without the need to remember them all.

Regularly update passwords

Set a reminder to update your passwords periodically. It is recommended to change them every three to six months or immediately if you suspect any security breach.

Remember, creating a strong password is an essential step in protecting your online security. By following these tips, you can significantly enhance the security of your accounts and reduce the risk of unauthorised access.

What is a data breach?

A data breach refers to an incident where unauthorised individuals or entities gain access to sensitive, confidential, or protected information. During a data breach, personal, financial, or other sensitive data may be accessed, stolen, or exposed without authorisation.

Data breaches can occur due to various reasons, including cyberattacks, hacking, malware infections, physical theft of devices or documents, human error, or vulnerabilities in security systems. The consequences of a data breach can be significant and may include financial losses, reputational damage, legal implications, and potential harm to individuals whose data has been compromised.

The effects of stolen passwords

The effects of stolen passwords can be quite severe and can lead to various negative consequences for individuals and organisations. Here are some of the potential effects of stolen passwords:

1. **Unauthorized Access:** Stolen passwords can provide attackers with access to various accounts and systems. Once the passwords are compromised, hackers can impersonate the account owners, gain unauthorized entry, and potentially perform malicious activities.

2. **Identity Theft:** Stolen passwords often go hand in hand with identity theft. With access to personal accounts, hackers can gather sensitive personal information, such as social security numbers, addresses, and financial details. This information can be used to commit identity theft, opening fraudulent accounts, making unauthorised purchases, or applying for loans or credit cards in the victim's name.

3. **Financial Loss:** If passwords associated with financial accounts, such as online banking or payment platforms, are stolen, attackers can gain access to funds and make unauthorised transactions. This can result in financial loss for individuals or organisations.

4. **Data Breaches:** Stolen passwords can contribute to larger-scale data breaches. If a user's password is compromised and they reuse it across multiple accounts, attackers can gain access to additional systems and databases, potentially exposing sensitive information of both individuals and organisations.

5. **Reputation Damage:** Password theft can lead to reputational damage, particularly if an individual or organization's accounts are used for unauthorised activities. The compromised accounts may be used to send spam emails, distribute malware, or engage in fraudulent activities, which can negatively impact the victim's reputation.

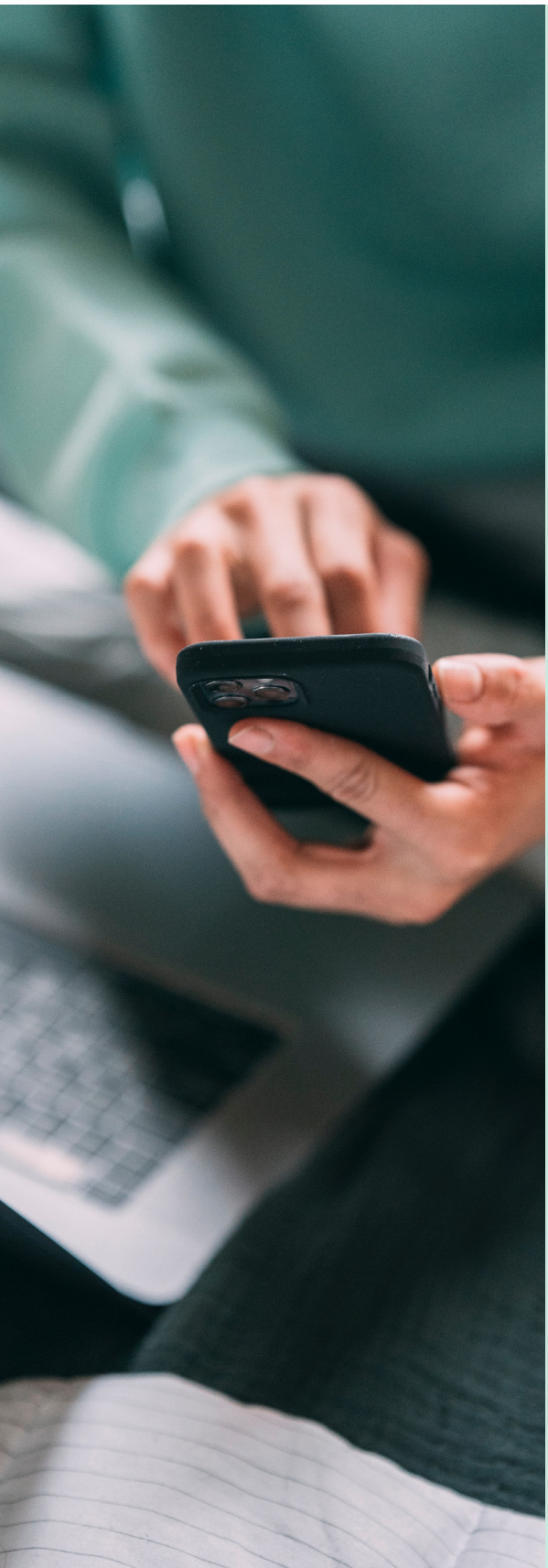
6. **Privacy Violation:** Stolen passwords can result in a significant breach of privacy. Attackers may access private messages, personal photos, or confidential documents stored within compromised accounts, leading to privacy violations and potential embarrassment or harm to individuals.

7. **Disruption of Services:** In some cases, stolen passwords can be used to disrupt services or systems. Attackers may change account credentials, lock out legitimate users, or engage in destructive activities that hinder the proper functioning of websites, applications, or networks.

To mitigate the effects of stolen passwords, it is crucial to practice good password habits including using strong and unique passwords for each account, enabling multi-factor authentication (MFA), and regularly monitoring account activities for any signs of unauthorised access. It is also essential to promptly report any instances of stolen passwords to the affected service providers and take necessary steps to regain control of compromised accounts.

How can passwords be hacked?

Passwords can be hacked through various methods and techniques employed by attackers. Here are some common ways in which passwords can be hacked:



1. **Brute Force Attacks:** In a brute force attack, hackers use automated software or tools to systematically guess passwords by trying all possible combinations. This method is time-consuming but can be effective against weak or short passwords.

2. **Dictionary Attacks:** Similar to brute force attacks, dictionary attacks use automated tools that systematically try a large list of common words or phrases as passwords. Hackers leverage pre-existing dictionaries or generate their own based on common words, phrases, or patterns.

3. **Social Engineering:** Social engineering involves manipulating individuals to reveal their passwords or other sensitive information. Attackers may impersonate trusted entities through phishing emails, phone calls, or messages to trick users into providing their passwords willingly.

4. **Phishing Attacks:** Phishing attacks involve tricking users into visiting fake websites or clicking on malicious links that mimic legitimate platforms. These websites or links often prompt users to enter their login credentials, which are then captured by the attackers.

5. **Keylogging:** Keyloggers are malicious software or hardware that record keystrokes on a user's device. When a user types their password, the keylogger captures it, allowing the attacker to retrieve the password later.

6. **Credential Stuffing:** In credential stuffing attacks, hackers use stolen username and password combinations obtained from previous data breaches. They try these stolen credentials on various websites or applications, knowing that many users reuse passwords across multiple accounts.

7. **Exploiting Weak Security Practices:** Attackers may exploit weak security practices, such as default or easily guessable passwords set by users, unsecured Wi-Fi networks, or poorly protected databases, to gain unauthorized access to accounts or systems.

Most popular passwords to avoid

Unfortunately, despite the increased awareness about password security, many people still use weak and easily guessable passwords. Here are some of the most commonly used passwords, which are highly discouraged due to their vulnerability:

- "123456" or slight variations like "123456789" or "12345678"
- "password"
- "qwerty"
- "1234567890"
- "1234567"

Useful Services and Websites

National Cyber Security Centre (NCSC) - Cyber Aware
The NCSC's Cyber Aware website offers guidance on password security, including tips for creating strong passwords and protecting personal information.

National Institute of Standards and Technology (NIST) - Password Security
NIST provides guidelines and best practices for password security, including recommendations for password composition and management.

StaySafeOnline - Password Security
StaySafeOnline provides tips on creating strong passwords, managing passwords effectively, and securing online accounts.

Have I Been Pwned
Have I Been Pwned is a popular service that allows you to check if your email address or username has been involved in any known data breaches. It provides information on which breaches your account may have been exposed in.

LSP's Safeguarding & Mental Health First Aider Teams

If you have any concerns at all, please don't hesitate to contact a member of our Safeguarding or Mental Health teams:

Safeguarding Lead: Andy Hamer
andy.hamer@learningskillspartnership.com
07526 168286

Safeguarding Officer: Anika Anwari
anika.anwari@learningskillspartnership.com
07432 840511

Safeguarding Officer: Fiona Sharples
fiona.sharples@learningskillspartnership.com
07447 799328

Safeguarding Officer: Yvonne Cogzell
yvonne.cogzell@learningskillspartnership.com
07710 70562

Admin/Chair & Safeguarding Officer: Kirsty Baggott
kirsty.baggott@learningskillspartnership.com
07809 342870

Mental Health First Aider: Fiona Sharples
fiona.sharples@learningskillspartnership.com
07447 799328

MORE INFORMATION

www.learningskillspartnership.com
info@learningskillspartnership.com