Protecting your personal information

Farm Advisory Service

National Advice Hub
T: 0300 323 0161
E: advice@fas.scot
W: www.fas.scot

Using online services is increasingly fraught with dangers as hacking and malicious attacks become more numerous and sophisticated. Simple password protection of data is now seen by many experts as a weak form of security and recommend using two tier security methods known as Two Factor Authentication (2FA)

What is Two Factor Authentication?

It is a security technique that requires two different methods to verify your identity when you log into a website. The first factor is usually something you **know** such as a user name and a password or a PIN, while the second factor is usually consists of something you **have** such as a mobile phone, but it could also be a USB dongle or other device that can generate one-time codes.

Activating the first factor e.g. inputting a password, user name, PIN etc. will trigger a request for the second factor, This may be a code that is sent via text to a mobile phone, via an App or a code generated by a device held by the person seeking to gain access. This latter method is often used by banks where a personal bank card is inserted into a reader that automatically generates a code that is recognised by the website.

Authentication Factors

There are a number of second factor authentication methods that can be use for Two Factor Authentication including:

- a physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
- a secret known only to the user, such as an encryption key, personal password, PIN, membership number etc.
- a physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
- somewhere you are, such as connection to a specific computing network or utilizing a GPS signal to identify

Security

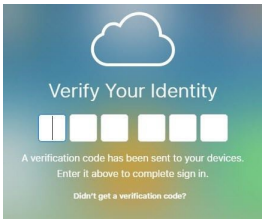
It is felt that two factor authentication (or multi factor authentication which requires several security steps) help to reduce online identity theft and other online fraud, because the thief requires more than just the victim's password.

However, many multi-factor authentication is still vulnerable to phishing, certain malware and interception attacks so good online security practice is still necessary.

Web services that use Two Factor Authentication include:

- Apple (iCloud and other services)
- Google (Gmail and other services)
- Microsoft Office 365
- Facebook
- Twitter
- Most bank
- UK Govt
- HMRC

Examples of Second Factor Devices



@FASScot

The European Agricultural Fund for Rural Development
Europe investing in rural areas

SAC CONSULTING

Scottish Government
Riaghaltas na h-Alba
gov.scot

Should I Use a Password Manager?

Farm Advisory Service
National Advice Hub
T: 0300 323 0161
E: advice@fas.scot
W: www.fas.scot

What is a Password Manager?

The majority of people use very weak passwords and use the same password across a number of on different websites. This is a risky practice but remembering difficult and numerous unique passwords that are easily forgotten can present its own set of problems. The solution to this could be to use a password manager.

Why Use a Password Manager?

Using the same password across many websites can create something called Password Leak, whereby a hack of one website can reveal your email address, username and password, which hackers can then try on other websites like your online banking or Paypal etc.

To prevent this possibility you need to use unique passwords for every website. These should be strong passwords or phrases – long, unpredictable that can also contain numbers and symbols. This can lead to difficulties in remembering all the unique login details for people using a large number of secure websites, which often means that they are written down, which is itself a further security risk.

A Password Manager will generates secure, random passwords for you and remembers them so you don't have to.

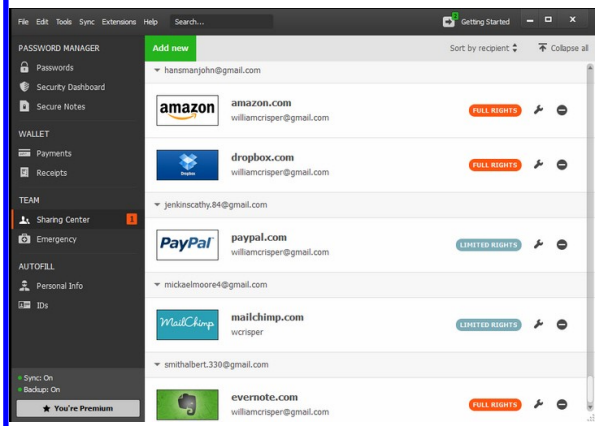
Using a Password Maanger?

When you visit a website that requires a login, instead of typing your password you open your password manager and type in your master password and it will automatically fills the appropriate login information into the website. (If you're already logged into your password manager, it will automatically fill the data for you). You don't have to think about what email address, username, and password you used for the website – your password manager does the dirty work for you.

If you're creating a new account, your password manager will offer to generate a secure random password for you, so you don't have to think about that, either. It can also be configured to automatically fill information like your address, name, and email address into web forms.

Which Password Manager Should I Use?

Most web browsers (i.e. Chrome, Google, Internet Explorer etc.) provide integrated password managers but they are not as good as dedicated password managers as they store the information on your computer in an unencrypted form, which could be vulnerable to hacking. Dedicated password managers encrypt your details and help to generate random passwords, when creating a new website account.



Well known dedicated Password Managers include Dashlane, LastPass and KeePass but there are many others also available, each with different attributes.

@FASScot

The European Agricultural Fund for Rural Development
Europe investing in rural areas

SAC CONSULTING

Scottish Government
Riaghaltas na h-Alba
gov.scot