Security of Your myDavy for Credit Unions Account

Introduction

At Davy we understand how important the security and confidentiality of your information is to you, and we are committed to our aim of ensuring that your interaction with us is done in a safe and secure manner.

This document will introduce you to the security features of your account, the steps you should take to protect yourself and will also give you an overview of some of the more common frauds and other identity theft issues that may threaten the safety of your account.

Davy has invested in security technologies and processes which are both visible and invisible to you, this section introduces you to those which are readily visible. In addition to these, in the background we have security features such as firewalls, logging and auditing systems, and regular audits of our security by both internal and external auditors.

Contact with Davy

Under no circumstances will Davy ever ask for your username or password in an email. If you receive such a communication, do not click on links or any attachments in the email and please contact Davy immediately.

Our website

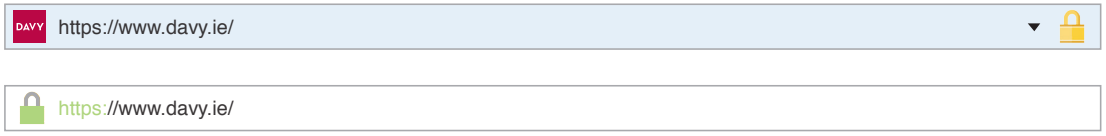
The only address you should ever use to log-on to Davy is **https://www.davy.ie.** Never go to this address from a link placed in an unfamiliar email or website and if unsure as to whether a communication is valid or a fake, type the address into the URL bar manually.

Encryption

Our website uses SSL encryption technology to ensure that communication between your browser and Davy is securely encrypted.

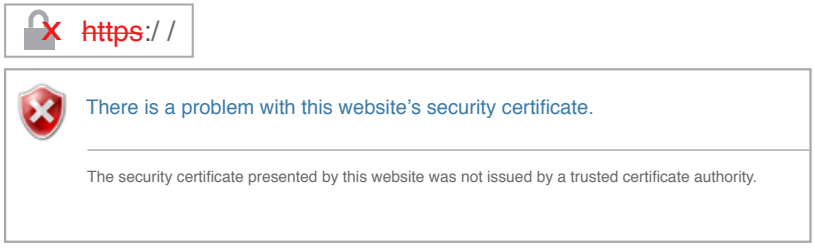
How to identify a secure page

When you are logging into myDavy for credit unions, and after you are logged in, the address should start with 'https://' and you should see a padlock icon in the address bar.



How to identify an unsecure page

If you do not see the **https://**, or if the padlock is missing or is replaced with some other icon (e.g. an icon with a red strike-through as below), you should not attempt to log-on.



Your username and password

The safety of your username and password is critical to ensuring the safety of your online account.

- Do not share your username and password with anyone.
- Do not re-use this password on other websites.
- If you think someone may have access to your password, please contact us on +353 1 614 9920 or at #CreditUnionSupport@davy.ie immediately.

We recommend you never allow your browser to save your username and password. If you have saved your details and would like to clear your saved information, please read below under 'Protecting my Password', How do I stop my computer from saving myDavy for credit unions username and password?

Logging Out

When you are finished, make sure to log out of myDavy for credit unions. A 'logout' link is provided on every page.

Contact Davy

If you are ever in any doubt about whether a communication is real, or if you have other concerns about your online account, please contact us on +353 1 614 9920 or at #CreditUnionSupport@davy.ie

Protecting your computer

Ensuring the security of your account requires both the protections we provide on our website, but it also requires you to ensure that your computer is secure. The following section gives you basic guidance on securing your computer.

Anti-virus, anti-spyware and firewall

The first step in securing yourself online is ensuring you have installed anti-virus, anti-spyware and firewall software from a reputable provider. As new viruses and other threats are constantly being developed, it is vital you continuously keep your anti-virus and firewall software updated by applying updates as they come available - nearly all anti-virus software can do this automatically so you don't have to worry about remembering!

Please ensure you only install anti-virus from reputable sources such as:

- McAfee: www.mcafee.com
- Symantec: www.symantec.com
- AVG: www.avg.com

Keep your system up to date

Operating system and browser vendors will typically provide regular updates which address newly discovered security issues. It is essential that you download these updates regularly. If your computer uses the Microsoft Windows operating system, keep it updated from the Microsoft website.

Be wary using computers you don't control

Having an online account makes it very convenient to access from any computer, anywhere in the world, which is not the same as saying it is a good idea to log into your account from any computer anywhere in the world. There have been news reports of computers such as those in WebCafes or Hotel Kiosks being found to be infected with "key-logger" viruses which record all usernames & passwords that are entered.

We do not advise you log into myDavy for credit unions from any computer other than one where you can assure yourself that the anti-virus protection is up-to-date, that it has been updated, and that no-one is monitoring what you are entering. You may wish to err on the side of caution when accessing myDavy for credit unions from third party computers.

Do not leave your PC unattended whilst logged-in

This advice applies if you are in a location where someone other than yourself may attempt to access myDavy for credit unions. Davy will automatically log you out if there is a period of inactivity, but logging-out yourself when finished is a more secure option.

Accessing from devices such as iPads, iPhones & Android

iPhone and iPad viruses are rare. Android devices are more susceptible to viruses, which are typically installed when malicious applications are downloaded. If you are concerned about the security of your computer, our current recommendation is the use of an iPad to access myDavy for credit unions.

Contact Davy

If you are ever in any doubt about whether a communication is real, or if you have other concerns about your online account, please contact us on +353 1 614 9920 or at #CreditUnionSupport@davy.ie

Frauds & identity theft

Unfortunately, there are fraudsters who may wish to try and access your financial accounts. This section will show you some of the more common frauds.

Remember, if you are ever in any doubt about whether a communication is real please contact us on +353 1 614 9920 or at #CreditUnionSupport@davy.ie

Phishing

Pronounced "Fishing", this is an increasingly common occurrence where attackers attempt to trick you into revealing sensitive information. Often these fraudsters will send an "official looking" email asking you to return sensitive information by email, or they will ask you to click on a link to visit a page where you will be asked for such information.

Fraudsters may also ask for such information via other channels, such as via unsolicited phone calls or SMS text messages.

Identifying phishing emails

These scams can be very sophisticated and often the emails are indistinguishable from real emails sent by the financial institutions.

- Any part of an email can be faked, including the 'From' address, text, any links and any attachments.
- Davy will never ask you to enter your username and password into any email.
- Davy will only ever ask for your username and password when you access https://www.davy.ie
- Phishing emails usually have a "call to action", i.e. an urgent request requiring you to take immediate action.
- The language used in phishing emails can often be unprofessional.
- The phisher almost always wants your username & login details, or your bank or financial account details. If in doubt, close the phishing site and visit www.davy.ie directly.
- Davy will only ever ask for your username and password when you access https://www.davy.ie
- Some phishing emails attempt to install viruses on your PC. If you see a request to install software, ignore it.

Only download anti-virus software from reputable vendors

A number of vendors of fake anti-virus software sell their products on the Internet. Typically these products offer to scan your system after you connect to a website, they inform you that they have detected a virus and they offer you their anti-virus software for a small cost.

When installing anti-virus, only install anti-virus software from a reputable vendor such as:

- McAfee: www.mcafee.com
- Symantec: www.symantec.com
- AVG: www.avg.com

Security of your email/webmail accounts

Should a fraudster gain access to your webmail accounts, they may attempt to impersonate you to financial firms and attempt to access funds in your account. Ensure that you have a strong password on your account, and do not re-use that password on other websites. Where possible, enable "two-factor authentication" (available for most of the major webmail providers.)

If you know or suspect your account has been compromised, notify any financial institutions who you have previously made contact with via email.

Social networking risks

Be wary as to the level of detail you post in public on social networking sites. Fraudsters have been known to collect and use information such as mother's maiden name, date of birth and employment details by monitoring social networking sites.

Fraudsters may also send out fake friend requests, or other messages which appear to come from a social networking site. Clicking on a link may bring you to a phishing website, or may lead you to a site where the fraudsters attempt to install a virus on your computer.

Postal mail security

Most financial institutions use postal mail to deliver some or all of your financial correspondence. Therefore, ensure that the address listed on your account is correct, and ensure as best you can that your postal mail cannot be intercepted. If you are changing address, ensure that your mail is redirected.

Where disposing of sensitive printed information, to avoid any possibility of identity theft it is recommended that you shred these documents.

Telephone frauds

There are a number of telephone based frauds/scams in operation. Davy staff will not ask you for your password over the phone, and if you receive such a request please notify Davy.

Common telephone frauds include the "tech support" caller, who will claim to be from some well-known computer firm (such as Microsoft) who is ringing to inform you that they have detected a problem on your computer. You may be asked to pay a fee for a "fix", or may be asked to download some software. Microsoft and other computer firms do not ring computer owners unannounced.

Useful websites

The following websites provide useful advice and tips for online security.

- http://www.makeitsecure.org/
- http://www.getsafeonline.org/
- http://www.safecard.ie/
- http://www.google.com/goodtoknow/
- http://www.eccireland.ie/popular-consumer-topics/scams/
- http://www.actionfraud.police.uk/fraud_protection/identity_fraud

The Davy Group is not responsible for the content of external websites.

Protecting your password

How do I stop my computer from saving the myDavy for Credit Unions username and password?

Some browsers and devices will prompt you to save your Davy password when logging on to myDavy for credit unions.

For security reasons, we recommend you never use this feature to store your Davy password. This is of particular importance when using a shared computer as someone else could access your information without your knowledge or permission.

If you have saved your Davy password and would like to clear your saved password data please follow the instructions relevant to your browser below:

- Internet Explorer
- Google Chrome
- Safari (Mac)
- Firefox

Two-Factor Verification

When you log-in on a Davy website, in addition to entering your username and password you will be asked to enter a verification code that will be sent to your mobile phone.

An additional layer of security

How it works:

1. Enter your username and password on the Login page
2. Your mobile phone will receive a code by text
3. Enter the code on the Login page

You are now logged in!

Remember

- The single-use code will be sent to the mobile phone number associated with your account.
- You have the option to click the 'remember me' button below the code field.
- This will allow you to login on the same device without the phone code for a period of 90 days.
- After this 90-day period has expired you will be required to enter a new code.

We strongly recommend you do not select this option on a device used by other people.

If you sign into myDavy for credit unions from another device, you will be asked to enter a new verification code sent to your mobile phone.

Contact Davy

If you are ever in any doubt about whether a communication is real, or if you have other concerns about your online account, please contact us on +353 1 614 9920 or at #CreditUnionSupport@davy.ie

Dublin Office Davy House, 49 Dawson Street, Dublin 2, D02 PY05, Ireland. +353 1 679 7788 dublin@davy.ie
Belfast Office Donegall House, 7 Donegall Square North, Belfast BT1 5GB, Northern Ireland. +44 28 90 310 655 belfast@davy.ie
Cork Office Hibernian House, 80A South Mall, Cork, T12 ACR7, Ireland. +353 21 425 1420 cork@davy.ie
Galway Office 1 Dockgate, Dock Road, Galway, H91 K205, Ireland. +353 91 530 520 galway@davy.ie
London Office Dashwood House, 69 Old Broad Street, London EC2M 1QS, United Kingdom. +44 207 448 8870 london@davy.ie
www.davy.ie/creditunions

107_24758/04/19