

Security

Information about protecting the assets in your Holding

WHAT IS THE BARE MINIMUM I MUST DO TO PROTECT MY HOLDING AGAINST UNAUTHORISED ACCESS?

There are three things you absolutely must do to protect your Holding:

- Always create a unique password (i.e., password)
- Keep your password secret
- Always access GoldMoney using a trusted computer

Create a Unique Password

Never reuse a password from another website, because it greatly increases the possibility of unauthorised access occurring in your GoldMoney Holding. Other websites may not protect the password you use to access them as well as GoldMoney does. By creating a unique password for your Holding, you protect against unauthorised access to your Holding if another website fails to keep your password secure.

Keep Your Password Secret

Never disclose your password to anyone because it increases the risk that your Holding may one day be accessed without your consent.

GoldMoney staff will never ask you for your password, so never disclose your password to anyone claiming to represent GoldMoney.

Finally, make sure you are really on the GoldMoney website before entering your Holding number and password on the login page. We recommend that you bookmark the login page in your browser for future access to your Holding:

<https://secure.goldmoney.com/user/login.php>

Always Use a Trusted Computer to Access GoldMoney

A trusted computer is a computer that you know is safe to use. Do not use computers at cyber cafes or other public establishments as they may contain 'keyboard sniffers' or other malicious software that can record your keystrokes and therefore steal your Holding number and password.

Your trusted computer should:

- have anti-virus and firewall software installed and regularly updated
- be regularly updated so that the operating system and installed software are always configured with the latest security and performance patches
- never use software or download files from or browse websites operated by a source you do not trust

If you think your computer has been compromised in any way, login to your Holding as soon as possible from another trusted computer and change your password immediately.

Security

Information about protecting the assets in your Holding

WHAT IS THE DIFFERENCE BETWEEN PREVENTING UNAUTHORISED ACCESS TO MY HOLDING AND PROTECTING AGAINST THE UNAUTHORISED REMOVAL OF FUNDS?

Providing access to your Holding and authorising the removal of funds from your Holding are two separate functions, and using a password to manage both of these functions is not really secure.

A password is useful to protect your Holding against unauthorised access. By keeping your password secret, you ensure that nobody else can login to your Holding to see the total value of metal and cash held in it or review the history of your past transactions.

But if there is no other security besides the password, there is nothing else to protect your Holding against the unauthorised removal of funds. This should be your fundamental concern, and GoldMoney provides you with a useful way to ensure that all removals of funds from your Holding are first authorised by you.

Many online systems attempt to secure accounts against the unauthorised removal of funds through the use of various security devices such as smart cards, “fobs” (keychain security devices), one-time passwords and other systems and devices designed to provide further protection than the simple username/password combination. However, all of these devices fall short in meeting both of these important requirements:

1. The security device must be a completely separate and unconnected piece of equipment from the computer accessing the account.
2. The security device must provide confirmation of any value transfer out of the account before the transfer is authorised.

GoldMoney addresses the issue of protecting the funds in your Holding by giving you the option to link your mobile phone to your Holding. Every time you attempt to either make a metal payment, to request for a delivery of a gold bar, or transfer cash from your Holding back to your bank account, you will receive a SMS text message on your mobile phone which includes the details of the transfer you are about to make and a PIN code that must be entered on the website to authorise the transfer. Once you have reviewed the details of the transfer, simply enter the PIN code into the website and the transfer is completed. Without the correct PIN code, the transfer will not be processed. Each transfer is assigned a unique PIN code of 7 alphanumeric characters, so the possibility of guessing a PIN is practically impossible.

This simple yet powerful protection works because it meets the two requirements listed above: (1) a separate device that allows you to (2) verify the value transfer instruction before authorising it on your computer. If the SMS text message showed a transfer instruction different than what you instructed and saw on your computer screen, all you would need to do is shut down the compromised computer and log into your Holding later from a secure computer and change your Holding’s password. Once you are running safely on a trusted computer, you could then initiate the payment or funds transfer instruction again.

Although no security method can ever be guaranteed to protect you 100% of the time, this method works very well because it requires that a criminal must compromise both your computer and your mobile phone in order to remove funds from your Holding. Compromising both of these devices at once is much more difficult than just compromising your computer.

Security

Information about protecting the assets in your Holding

HOW DO I CHANGE MY PASSWORD?

You can change your password after you have logged into your Holding by clicking the 'Security > Change Password' link and then entering a new password. We recommend that you change your password periodically to help protect against unauthorised access to your Holding.

Security

Information about protecting the assets in your Holding

WHAT CAN I DO IF I LOSE MY PASSWORD?

First go to our [login page](#).

Then click on the 'Request a New Password' link next to the password entry box. Follow the instructions provided to initiate the issuance of a new password.

Depending on the amount of value held in your Holding, a GoldMoney customer service representative may contact you to confirm your request.

Security

Information about protecting the assets in your Holding

WHY AM I LOGGED OUT OF MY SESSION WITH GOLDMONEY IF I DON'T DO ANYTHING FOR AWHILE?

This feature is implemented as a security measure to safeguard your Holding. GoldMoney limits the amount of time that your session is held open if there is no activity. After one hour you are automatically logged out of your Holding, and your session with GoldMoney is terminated. You must then log in again in order to access your Holding.

Security

Information about protecting the assets in your Holding

I RECEIVED AN EMAIL FROM AN ADDRESS AT GOLDMONEY.COM WITH AN ATTACHMENT. SHOULD I OPEN THE ATTACHMENT?

No, never download and/or open such an attachment. GoldMoney will never send email with an attachment.

Criminal hackers often send out emails that appear to be sent from a trusted party but are actually sent from the hackers themselves (this technique is called 'spoofing'). Unfortunately, the limitations of email software make these spoof emails possible.

The attachments often contain malicious programs called 'trojans' designed to steal personal information stored on your computer or to log your keystrokes and steal passwords. If stolen, this information would give the hacker access to your GoldMoney account and your money. Attachments from a spoofed address may also contain computer viruses designed to cause havoc on your computer.

To repeat this important point, never open an attachment sent to you from any email addressed from goldmoney.com. Immediately delete the attachment if downloaded onto your computer.

Security

Information about protecting the assets in your Holding

I RECEIVED AN EMAIL FROM AN ADDRESS AT GOLDMONEY.COM WITH A HYPERLINK (WEB ADDRESS) EMBEDDED IN THE EMAIL. THE EMAIL ASKS ME TO LOG INTO MY HOLDING. IS IT SAFE TO CLICK THE HYPERLINK AND LOG INTO MY HOLDING?

No. GoldMoney will never, under any circumstance, send an unsolicited email asking you to login to your Holding by clicking on an embedded link.

Criminal hackers often send out emails asking for the recipient to login to what appears to be a trusted online financial account. Although the emails appear to be sent from the financial institution, they are actually sent by the hackers themselves in a technique called 'spoofing'. Malicious hyperlinks usually direct the recipient to a site that appears to be the trusted financial institution, but is actually a website set up by a hacker for the sole purpose of stealing your personal information, including your login ID and password. If stolen, this information would give the hacker access to your account and your money.

Often, the hyperlink presented in the email looks exactly like the site for which the hacker is attempting to steal your login details. For example, it may say: 'Go to goldmoney.com to login to your Holding to verify information'. However, clicking the link will actually take you to the spoofed site run by the hacker.

GoldMoney will never send you an email with embedded hyperlinks to the login page, with the sole exception being the confirmation email that is sent to you when you first create a Holding.