ForgotIt? 2.5
User Manual

by Erich H. Rast, Ph.D.

ForgotIt?

... never forget it again!

Contents

1 Introduction

ForgotIt? is a password reminder application that uses a combination of the Blowfish, Advanced Encryption Standard (AES) and Camellia ciphers to protect password lists against unauthorized access. SHA-256 and Ripemd-160 are used as secure hashing algorithms.

The Mac OS X and Windows versions of the program are shareware. If you continually use the application on these platforms you *have* to pay the shareware fee. By installing *ForgotIt?*on your machine and using it you agree to the end-user license agreement (Appendix I on page 39). Please read it!

The GNU/Linux version is gratis, i.e. you do not need to pay the shareware fee if you are only using *ForgotIt?* on GNU/Linux.

1.1 What's New?

Version 2.5 improves stability on Mac OS X 10.10 ("Yosemite"), now checks for well-known passwords in the password dialog, improves the Window menu, and adds a context-menu in the main list view and in the edit dialog that allows you to copy entries to the clipboard.

1.2 Platform-specific Issues

ForgotIt? is available on common distributions of GNU/Linux, Mac OS X, and Windows. This manual is for all versions. Database files are cross-platform. The behavior of the application itself may differ slightly from operating system to operating system. Most of these differences only concern the look and feel or platform-specific controls of common user interface elements. Whenever there is a more substantial difference it will be mentioned in this manual.

The screenshots in this manual were made on Linux running XFCE with default compositing window manager and the 'Greybird' theme. On your machine dialogs and windows will likely look different and might use other icon sets. Dialogs have their native look and feel on each platform, and their look also changes from version to version of each operating system. Most operating system configurations also determine or influence the way

windows show up and stack on the screen when they are opened for the first time.

1.3 Abbreviations Used in this Manual

Different operating systems use slightly different keyboard layouts and names for keyboard shortcuts. In what follows, Cmd stands for the command key on OS X and the control key on Linux and Windows. For example, the menu command for opening a new document Cmd O stands for pressing the command key (control key on Linux and Windows), keeping it pressed and pressing the key of the letter 'o'. Alt stands for the key that is (usually) called *Option* key on OS X and *Alt* on other keyboards. On Linux it appears as *Meta* key in menu shortcuts.

2 Installation

2.1 System Requirements

Mac OS. As of version *ForgotIt?* 2.5 for Mac OS X requires a minimum of 2 GB RAM and OS X version 10.4 or higher running on an Intel processor. For smooth functioning, 4 GB of RAM or more are recommended. Older Macs based on the PowerPC architecture are no longer supported.

GNU/Linux. *ForgotIt?* should work on most recent distributions with Linux 2.6 kernel and a machine with 1 GB RAM or more. The following dynamic libraries need to be installed: libglib-2.0, libgmodule-2.0, libgobject-2.0, libpango-1.0, libpangocairo-1.0, libcairo, libjpeg, and libpng12 or libpng. *ForgotIt?* has only been tested on Ubuntu 12.04 LTE.

Windows. Windows XP, Windows Vista, or Windows 7 with at least 4 GB RAM and an Intel Core i3 processor or better are needed.

2.2 How to Install

Mac OS X. To install *ForgotIt?*, mount the disk image containing the application (usually named 'ForgotIt.dmg') by double-clicking on it if it hasn't been mounted automatically already. Locate the volume called 'ForgotIt2',

open it, and drag & drop the *ForgotIt?* application to your 'Applications' folder or any other folder you want it to reside in. Depending on where you copy the application to you might have to identify yourself with a valid admininstrator name and password during this process.

If you don't have access to the administrator account on your machine, you may also install *ForgotIt?* in a folder in your user's home directory. For example, you may drag and drop the application into a folder named 'Applications' inside your home folder. In this case, other users on the same machine will not be able to use the application.

GNU/Linux. *ForgotIt?* comes as a .zip archive. You may unpack the archived files to any directory and the application should work out of the box provided the necessary libraries are installed (see previous section). To launch *ForgotIt?* start the program 'ForgotIt2' in the directory 'ForgotIt2/bin/' or create a menu shortcut or custom launcher for the executable. There are application icons in the following relative path:

```
ForgotIt2/lib/plt/ForgotIt2/exts/ert/racket/collects/icons/
```

Windows. A standard installer will guide you through the installation process. When it has finished successfully *ForgotIt?* should reside in the program directory you have chosen and can be launched by double-clicking the application icon.

2.3 Technical Datasheet

Product Name:	Peppermind *ForgotIt?* Password Manager
Product Version:	2.5
Specification:	small encrypted free-text database
Distributor:	peppermind.com
Platforms:	Windows XP, Vista, 7; Mac OS X 10.4-10.9°; GNU/Linux 2.6
Max. Memory:	dynamic*
Max. Item Size:	dynamic*
Max. Items:	dynamic* (less than 3000 recommended)
Max. Categories:	dynamic* (7 or less recommended)
Max. Fields:	12 per category†
Text Format:	UTF-8, binary data Base64 encoded
File Format:	XML
Encryption:	3-pass encryption using Blowfish, AES, and Camellia
Hashing:	iterative SHA-256 and Ripemd-160 with additional key-stretching

*limited by available system memory; °certified only for OS X 10.6; †soft limit; can be changed by preference key `fields-soft-limit`

3 The User Interface

ForgotIt? has a standard multiple-document interface that allows you to view and edit several databases at once. Upon launching the application for the first time, it might ask you to re-enter some of your registration information provided a registered earlier version is detected. Then it opens a new, untitled document. Whenever *ForgotIt?* is launched subsequently by directly clicking on the program icon or starting it from the command line, it will ask you to open an existing password list. If you press Cancel in this dialog, a new untitled document is opened.

Windows generally remember their size and position, but changes to their state are only made permanent if the document content has been modified and the document is saved. If you wish to reset a window's size and position to its default state, press the Shift key while opening the window.

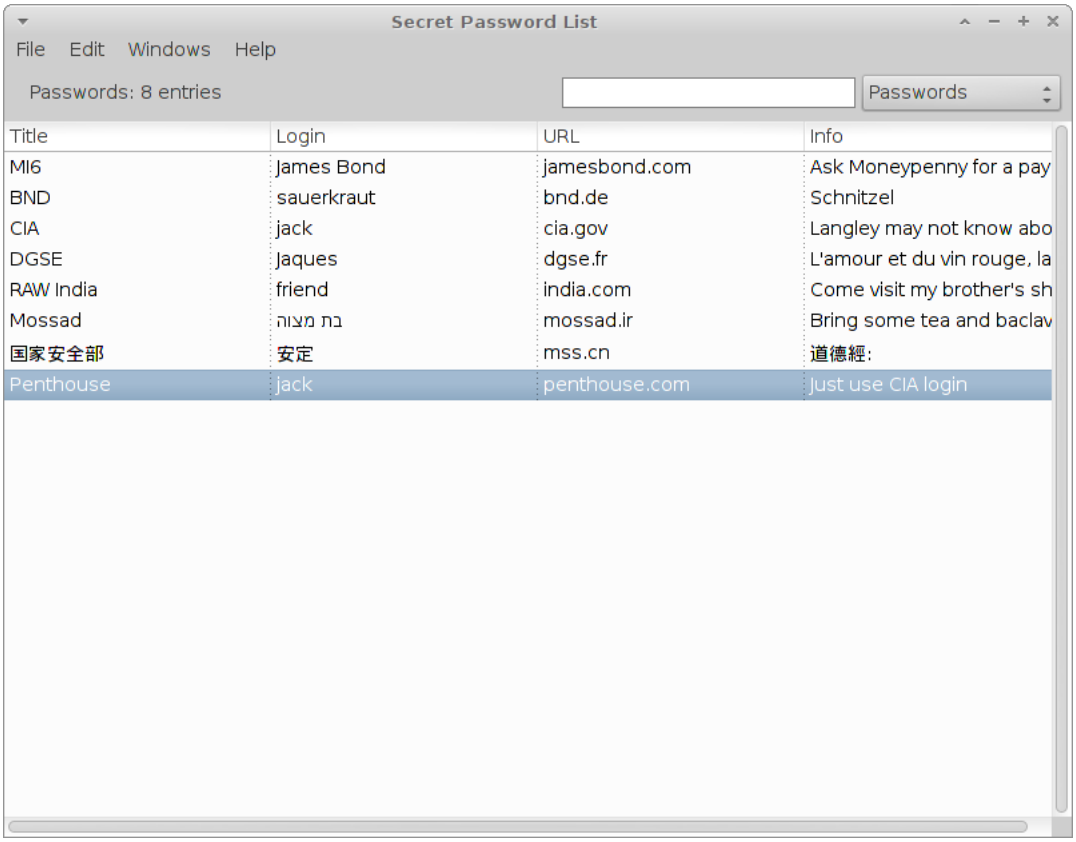

Figure 1: The main list view.

3.1 The Main Window

The main window displays information about the currently selected category, a quick search field, and a category selection menu on top of the window. At the larger bottom of the window is a list view of all entries of the currently selected category (Figure 1).

Navigating the Main List. When the main list is selected, you may move through the entries using the up and down arrow keys or the scroll wheel of your mouse. You may view the edit dialog of an entry by double-clicking

on it or pressing the Enter key.

Re-ordering and Re-sizing Columns in the Main List. Columns in the main list can be re-sized by clicking between the header entries and moving the mouse while keeping the left mouse button pressed. Whole columns can also be re-ordered by grabbing their headers with the mouse (press left mouse button and keep it pressed) and dragging them along the list headers to their new location. The new size and position is saved permanently only when the content of the document has been modified and is saved.

Searching for Items. To search for an item in the list, select the search field on top of the window by double-clicking on it and enter the search term. The list of entries found will be updated while you are typing. All fields of an item except password fields are searched. Delete the content of the search field by selecting it and pressing Backspace to return to the full list view.

Changing the Category. To change the category displayed, choose a category from the category on the top left corner of the window. You may also move through the categories by pressing Cmd → and Cmd ← on the Mac (Cmd] and Cmd [on Linux and Windows).

Basic Editing. You may select an item by clicking on it. To move through the list, you may use the arrow keys ↑ ↓ or the scroll wheel of your mouse. Pressing Shift while selecting items extends or shrinks the selection respectively. To view or edit the currently selected items press Return. To delete the currently selected items press Backspace. Standard copy and paste commands are also available and described in more detail in the next section.

Context Menu. Right-clicking an item in the main list view will display a context menu that allows you to copy associated data such as the password to the clipboard without opening the item for editing. *ForgotIt?* deletes this data from the clipboard when the application quits, so it needs to be running and open before pasting the contents of the clipboard into the editor window of another application such as a web broser.

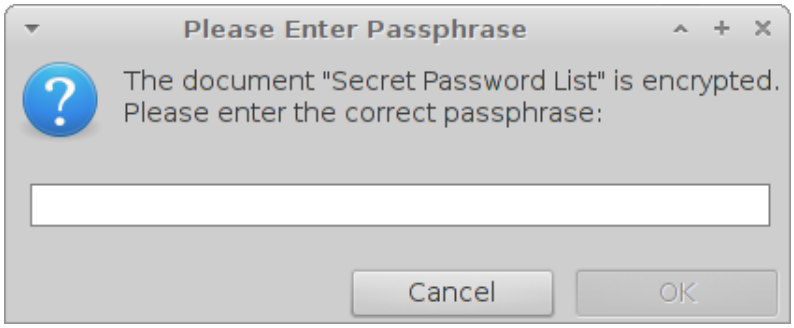

Figure 2: Entering the passphrase to access an encrypted database.

3.2 Opening and Closing Documents

Opening an Existing Document. By default you are asked to open an existing document when the application is launched by double-clicking on its icon after the first program launch. You may also open a document by double-clicking on its program icon or by choosing *Open* Cmd O from the *File* menu. On Linux you may need to choose the 'ForgotIt2' binary executable at the path where it has been installed the first time you open a database document by double-clicking on it. In some cases, you might also need to specify the application executable manually by providing the full path to it.

When the database is encrypted, a passphrase dialog will show up (Figure 2) into which you have to enter the correct passphrase. Once you have entered the correct passphrase and pressed Enter, the document will be opened in a main window displaying the list view (category and other display state) under which it has been saved the last time. Attempts to open a database with the wrong passphrase are logged (see section 3.6 on page 23 for more information). By default the application quits after three incorrect attempts to open an encrypted database unless another database is already open.

Quitting the Application. *ForgotIt?* behaves in a slightly different way than normal applications on OS X, similarly to how a *control panel* used

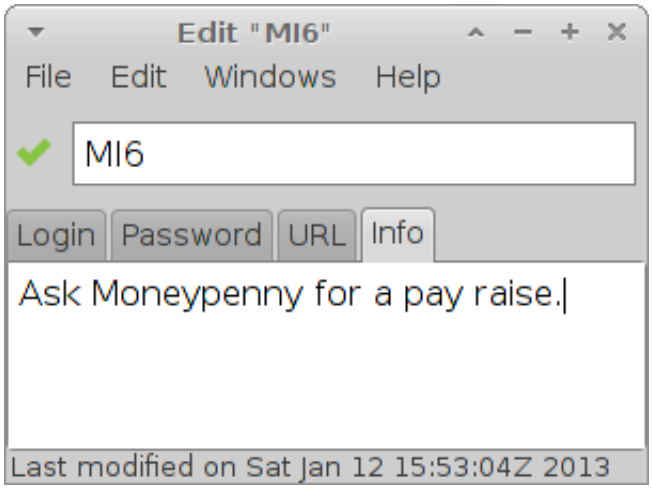

Figure 3: An edit window.

to work on Classic Mac OS. By default the application quits when the last main document window has been closed. This is the default behavior on Windows and also how most Linux applications behave.

As usual, *Quit* Cmd Q from the *File* menu quits the application. If you have made changes to open documents, you will be asked to save them before the application quits.

3.3 The Edit Window

Individual items are viewed and edited in edit windows (Figure 3). For each item one edit window is opened when it is selected for viewing or editing. The first field of the entry is always given as a title line in this window. All subsequent fields can be selected by a tab panel below this field.

Index Field Status Indicator. Starting from *ForgotIt?* version 2.0 one or more fields of a category may be *index fields*. Usually the first field of a category is an index field. As opposed to other types of fields an index field needs to be non-empty and its value must be unique within that field's values of all items of that category. The icon next to the title field of

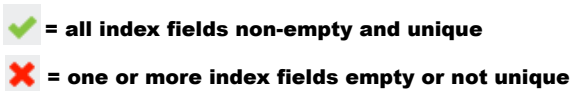

Figure 4: Index field status indicator in edit windows.

an edit window displays a large red cross when these conditions are not fulfilled for one or more index fields of the given item; otherwise it displays a green checkmark (Figure 4). When defining your own categories, it is recommended to make the first field of a category an index field. See section 3.4 on page 15 for more information.

Navigating through the Window. Pressing the Tab key navigates through the fields of the item. Pressing Alt Tab navigates in the opposite direction.

Basic Editing. Standard commands for text editing are available in the edit window. These are described in more detail in the Command Reference (section 5 on page 31).

Context Menu. Right-clicking a non-editable area in the dialog will display a context menu that allows you to copy data such as the password to the clipboard without switching to this entry first. *ForgotIt?* deletes this data from the clipboard when the application quits, so it needs to be running and open before pasting the contents of the clipboard into the editor window of another application such as a web broser.

Viewing the Creation and Modification Date. By default an edit window displays the date when the respective item was last modified. By clicking anywhere on the window outside of an edit field, for example on the red cross or green checkmark icon, the creation date of the item will be displayed. Another click outside the edit areas displays the modification date again.

Updating Changes in the Main List. For performance reasons changes made to an item in the edit window do not immediately become visible

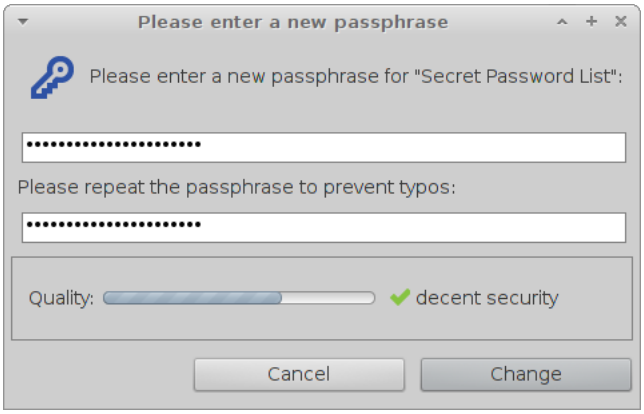

Figure 5: A Passphrase dialog with a good passphrase estimate.

in the main list. The main list are updated automatically when (i) the corresponding edit window is closed, (ii) the main list window is closed, or (iii) the application quits.

Window Position and Size. Edit windows remember their position and size automatically. However, this information is only saved when some text has been changed as well.

3.3.1 Setting or Changing the Passphrase

By selecting *Set Passphrase...* Cmd K in the main window, the passphrase dialog is opened in which the passphrase for the document can be set or changed (Figure 5).

Navigating through the Window. You may navigate between input fields using the Tab key or by selecting the edit fields with the mouse.

Entering the Passphrase. To safeguard against accidental typos you must enter the passphrase twice. Passphrases are case-sensitive and may contain special characters. While you enter the passphrase a quality estimate is displayed in the field below the input fields. A passphrase can only be

changed when it has the minimum length as specified in the Preferences (see Section 3.5 for more details) and the two passphrases entered are exactly identical. To confirm the change, press the *Change* button or Enter. To cancel the action, press the *Cancel* button or keystrokeEsc.

Choosing a Good Passphrase. A good passphrase must be long—at least 8 characters and ideally 20-30 characters—, contain numbers, upper- and lowercase letters, and special characters like punctuation. However, it is also very important that you are either (i) able to remember it in the long run or (ii) note it down and keep it in a place that is entirely safe. Both choices have their advantages and disadvantages. This issue and more general security considerations are discussed in section 4. As a rule of thumb, relatively safe passphrases can be obtained from modifying nonsensical phrases with additional characters and punctuation. Notice that the security estimate given in the passphrase dialog is really just an estimate: The application does currently not use a dictionary to check for long and seemingly complicated but nevertheless easy to guess passphrases.

Note: *Starting with version 2.5 or higher, ForgotIt? does not allow you to use a passphrase that is among the 10,000 most commonly used ones.*

3.4 The Category Window

Starting with *ForgotIt?* 2.0, categories with different field names and field content can be defined and changed by the user. Current support for categories is fairly limited, though, and some care needs to be taken when designing your own categories. Since changing categories and their fields can require (voluntary) deletion of data and data cannot easily be transferred between fields, it is recommend to define categories and their fields once prior to entering any actual data.

Categories are changed in the Category Window available from *Edit Categories...* Cmd Alt K in the*Edit* menu (Figure 6).

Reordering Categories. The order in which categories appear in the category menu of the main window can be changed by selecting a category whose order is to be changed by clicking on its name with the mouse in the list, and then pressing the *Down* and *Up* buttons to move it in the list.

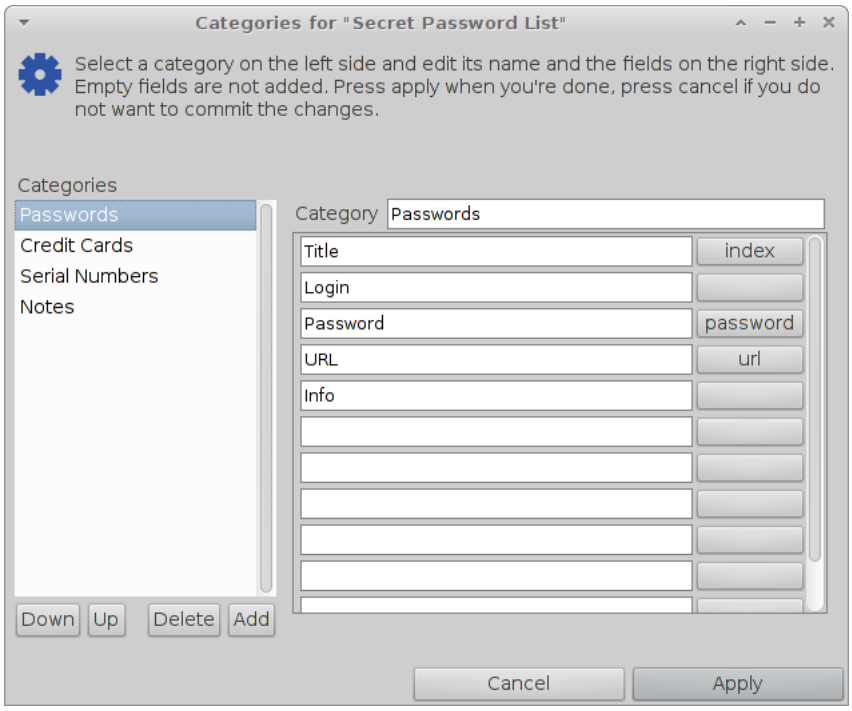

Figure 6: Categories are edited in the Category Window.

Deleting a Category. When a category is deleted, all items of that category are deleted and the corresponding information is lost. So please be careful with this function! To delete a category, select its name in the list to the left and press the *Delete* button.

Creating a New Category. A new 'untitled' category is created by pressing the *New* button. The title of the category and its fields can be edited on the right side of the window as described in the next paragraphs.

Editing the Name of a Category. After the label 'Category' an edit field allows you to change the name of the category. Names of categories must be unique within the document. Changing the name of a category is a harmless operation, because it does not otherwise affect its content.

Editing Fields of Category. When a category is selected in the list on the left side of the window, its fields are listed below its name on the right hand side together with information about the field type. Editing fields of a category works as follows:

Changing the Name. The name of a field is simply changed by editing it in the corresponding edit field. Changing the name of a field does not affect any other data stored as long as the name remains a valid sequence of alphabetic characters. Special characters or spaces are not allowed in category or field names.

Deleting a Field. A field is deleted by deleting all characters of its name in the edit field. *Caution:* Once it is confirmed (see below) this is a highly destructive change, as all data entries of that field in all existing items of the category are deleted when the field name is deleted. The resulting category will simply leave out the respective field and it will be deleted from all items of that category.

Adding a Field. A field can be added by simply filling its name into an empty field below the existing ones. This is a non-destructive change, since it only adds an additional empty data slot in all items of that category.

To summarize, changing the name of a field and adding a new field are innocuous operations, whereas care should be taken when deleting fields by giving them an empty name.

Field Types. Behind the name of a field is a button indicating its type. A field's type can be changed by subsequently pushing this button, which will cause it to cycle through all its possible type values. The meaning of the types displayed on the button are as follows:

no label This is the standard type. The field holds arbitrary text.

index The values of all index fields of an item must be non-empty and unique (for that field) within all items of that category. The first field ('Title') of a category should be an index field. When an entry is edited and a duplicate value is given to an index field, *ForgotIt?* will automatically add a number to it in order to ensure its uniqueness once the entry is updated in the main list. When an entry is edited and an index field is left empty, *ForgotIt?* will automatically create a unique name for it once the entry is updated in the main list.

url An URL field is designed to contain a list of URLs, each of them on a line of its own. While other fields may also contain URLs that can be launched by double-clicking on them, the *Launch URL...* Cmd L command of the *File* menu launches only the URLs stored in URL fields of an entry.

password A password field is hidden in the main list and supposed to contain a passphrase or similar secret information. Each category should only contain one password field, although this restriction is not enforced in the current version. For now, there is not much of a difference between a hidden and a password field. Future versions of *ForgotIt?* may handle password fields differently from other fields in various ways, e.g. they might not echo characters and instead only display bullets like in the passphrase dialog.

hidden A hidden field is a normal text field that is not displayed in the main list. Currently, it works much the same as a password field but it should be chosen when the field does not represent a passphrase of

any kind. A category may contain more than one hidden field but in total at least one field of a category must be visible.

Consistency Checks. Changes made in the Category Window will only be applied after pressing the *Apply* button and you will be asked for additional confirmation upon requesting certain destructive changes like deleting a field or a category. Additionally, *ForgotIt?* performs a variety of consistency checks on the fly. If the *Apply* button is not enabled, the check has not been passed. This happens for instance when a field name contains illegal characters, when all fields of a category are invisible (at least one field must be visible), or when a category has no field at all. In that case, some small information about the problem is displayed above the section on the right hand-side of the window.

Note: *Please be careful when editing categories. Press* Cancel *if you have made a mistake to discard the changes you have made in the Category Window so far. If you have inadvertently applied a destructive change to an existing document, revert the operation immediately by choosing* Undo Cmd Z *from the* Edit *menu. Use backup software and always make incremental backups of your documents (OS X Time Machine is your friend). Because of the limitations of the current implementation of categories, e.g. you cannot save templates or easily move data between categories or fields, I recommend to edit the categories of a document only once in the beginning before any actual data is entered.*

3.5 The Preferences Dialog

The preferences dialog allows you to change global settings. Changes made here affect the whole application and all documents that are opened by it (Figure 7).

You can select different sections by clicking on section headings in the upper part of the tab panel. In what follows, all settings are listed and described under the section in which they occur.

- General
  - Print font family: This setting determines the font used for printing documents. Only the generic font family can be adjusted here

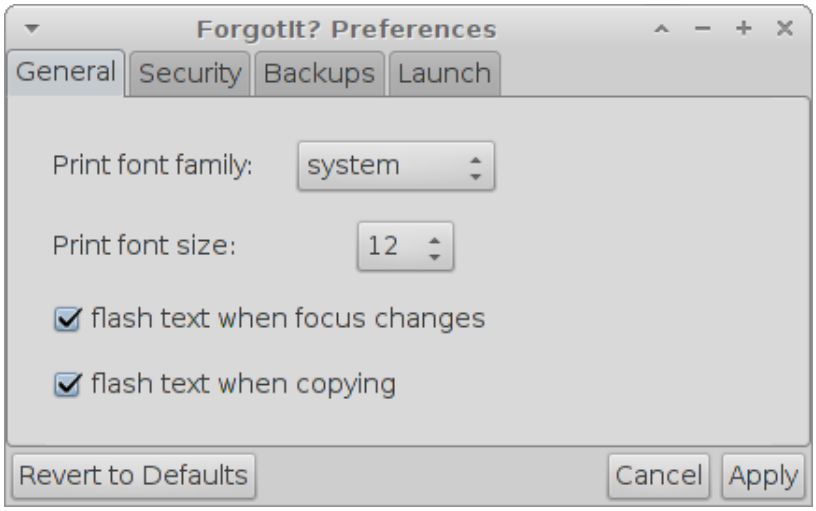

Figure 7: The preferences dialog.

and the actual font values for each family are hard-wired into the application. (This might change in future versions. In any case printing is insecure and documents should only be printed if absolutely necessary.)

- Print font size: Here you may choose the size of the print font in points. Various steps from 7 pt. to 64 pt. are supported.
- Flash text when focus changes: When this option is checked, the text in edit dialogs flashes briefly when you tab through different fields.
- Flash text when copying: When this option is checked, text that is copied into the clipboard is flashed for a short time in order to indicate that it has been copied.

- Security
  - Minimum passphrase length: The menu allows you to vary the minimum required passphrase length of a document passphrase between 3 and 32. If an attempt is made to set a passphrase

shorter than the minimum passphrase length then the passphrase is not accepted in the Change Passphrase window. The default value of the setting is 6, but you might want to set this higher. A safe master passphrase should have at least 12 characters. (See section 4 on page 23 for more details.)

- Warn before insecure actions: When this option is checked, you are warned whenever you attempt to perform some operation that is inherently insecure, giving you the opportunity to cancel the operation. For example, printing documents or exporting them in an unencrypted format are insecure actions. It is recommended to leave this option always on.
- Log level: From the menu the level of detail with which the application's log file is written may be chosen. The log contains information about errors or security relevant events that occurred such as attempts to open a document with the wrong passphrase. (See section 3.6 for more information.) The default level 'warnings & errors' should be adequate for most purposes.

- Backups
  - Automatically write backups: When this option is checked, when a *ForgotIt?* document is saved to disk and overwrites an older version a copy of the old version is made either in the same directory (if the custom backup directory option is not checked) or in a directory chosen by you in case the custom backup directory option is checked and a valid directory has been chosen.
  - Maximum number of backups: In this field the maximum number of backups per document can be adjusted. The default value is 3, because *ForgotIt?* backups are only meant as an additional safety measure, not as a replacement for custom backup software.
  - Custom backup directory: When this option is checked, a custom backup directory may be selected by pushing the *Choose* button. When a document overwrites an old document, the old document is renamed according to a fixed renaming scheme containing the date and a unique identifier and then copied to the custom backup directory. Please note that the custom backup directory

must be writable and available at all times—so, for instance, it may not reside on a mountable volume.

Note: *ForgotIt?'s automated backups are only intended as an additional safety net and can fail for a variety of reasons. It is highly recommended to regularly make backups using 3rd party tools regardless of ForgotIt?'s backup settings. My general advice is to backup important documents often and regularly. For example,* CrashPlan *offers reliable and fully-automatic cross-platform backups at a fair price. (I'm not paid for saying this; it's just a recommendation based on personal experience.)*

- Launch
  - Open default database: When this option is checked, *ForgotIt?* will open a user-defined database on program launch, prompting you for the password. Choose a default database by pressing the *Choose* button.
  - Remember queries between project launches: When this option is checked, *ForgotIt?* will remember the last query that was entered into the search field. Since many users found this option confusing, it is switched off by default since version 2.3.
  - Check online for new versions: When this option is checked, *ForgotIt?* will check for new versions of the application on each program launch and inform you of new versions. No private information is transmitted by the version check, it simply downloads via HTTP a small version information text in UTF-8 format from `http://13874.website.snafu.de/versions/forgotit`. The application does not attempt to make any kind of incoming or outgoing connection if this option is switched off unless you instruct it manually from the *Help* menu to check for a new version.

Note: *The default database option is a residue of ForgotIt? 1.4 and I currently do not recommend you to use it. It is much better to open your preferred document by double-clicking on it instead. On OS X and Windows documents can also be put instead of applications in many places like for example as start items. To launch a document from the command line interface you may use the* `open` *command on OS X and* `xde-open` *on Linux.*

3.6 The Log

The log is a file in which *ForgotIt?* protocols security-related events such as errors or attempts to open documents with the wrong passphrase (Figure 8).

You may save the log by pressing the *Save* button, which will open a standard save file dialog, and you may print it by pressing the *Print* button, which will open a platform-specific printer dialog.

4 Safety Considerations

ForgotIt? is primarily a password reminder program and so a few remarks about security and password safety are appropriate.

4.1 Things to Consider

There is no such thing as prefect safety or perfect security. When musing about the security of an encryption system or the safety of your confidential data, you need to be aware of some trade-offs.

The Most Likely Attack. Bear in mind that the most likely attack on a *ForgotIt?* database will be a *side-channel* attack and not an attack on the actual encryption of the document. Potential side-channel attacks, ordered by decreasing likelihood: a trojan or virus that installs a software keystroke logger (preferred tool of bosses/hackers/ acquaintances/ex-lovers, etc.); a hardware keystroke logger (often used by law-enforcement, although they seem to move to software methods in some countries; can be bought at any Chinese wholesale site so it might also be used by private citizens); a hidden camera installed in your apartment (used by law enforcement, intelligence agencies); a Van Eck device (probably only used by intelligence agencies). Don't bother with bugs and Van Eck devices—protection against them is almost impossible for a private citizen and requires equipment whose use is illegal in many countries. If you consider it possible that someone might use such equipment against you—say, you have some trade secrets and suspect heavy industrial espionage—you probably ought to hire an experienced security consultant or contact the responsible authorities. Defense against the other, more mundane attacks requires keeping the software up to date

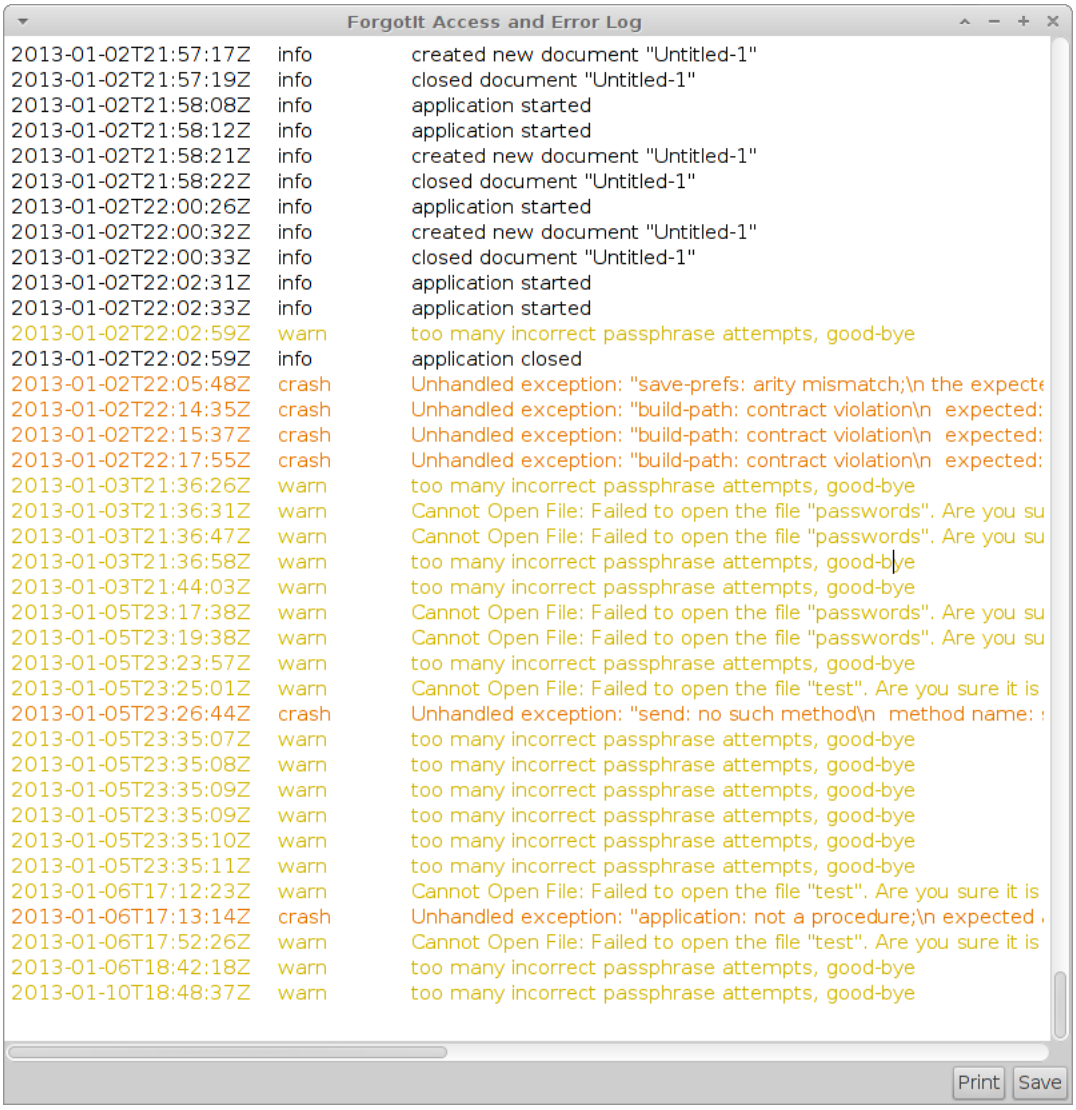

Figure 8: The log dialog where security-related events are protocolized.

and the computer physically secure (see below). Finally, another effective side-channel attack needs to be mentioned:

```
http://xkcd.com/538/
```

Solution: Avoid the guy with the wrench.

Data Integrity versus Security. Encryption generally decreases data integrity, because when encrypted files are damaged it is much harder to recover their original content than that of ordinary files. Tight general security measures and procedures also tend to decrease data integrity, since for instance example a policy not to make copies of sensitive data, which might make sense from a purely security-related perspective, may increase chances of fatal data loss in case of technical failures. Therefore, data integrity (keeping the data) and security (keeping the data away from prying eyes) must always be considered in combination. Don't lock yourself out by choosing passphrases you cannot remember and make frequent backups of your important data. In some cases it can make sense to write down the master passphrase and keep it in a safe place such as your wallet or a bank safe.

Usability versus Security. Higher security generally goes hand in hand with a decrease in usability. For example, requiring passphrases to be at least 12 characters long is more secure than setting the minimum length to 6 characters provided you can remember the longer master passphrase or have a safe place to store it. To give another example, encrypting data on the basis of two separate passphrases can be much more secure than encryption with just one, but having to remember and enter two passphrases might be too cumbersome for many users. A third example is automated passphrase expiry: Forcing the user to change the passphrase in regular intervals can increase security, because it decreases the amount of time an attacker has to exploit the system in case he has successfully compromised it and forces him to constantly renew his attack, which makes it in turn easier to detect. However, passphrase aging can become very annoying to users when they have to manage dozens of different passphrases for dozens of different sites or systems, which can result in people using trivial passphrases.

Security versus Security. This might sound strange at first, but too high security may also defeat its own purpose. Consider the examples mentioned in the last paragraph again. Suppose an application would force you to use a master passphrase of at least 32 characters. You would likely end up scribbling the passphrase on a piece of paper. Depending on where you keep it, this could result in an overall decrease in security in comparison to allowing shorter passphrases that you can remember. Similar things sometimes happen in companies when very strict security measures are in place. Whenever security gets too much in the way of usability, people tend to show great ingenuity at circumventing it. Likewise, too high security at the cost of data integrity can make denial of service attacks feasible. To cut a long story short, security measures must be weighted against other factors as dependent on the expected attack scenarios in order to be able to implement them efficiently. Never believe in unconditional security claims or claims about 'military-grade security.'

What trade-offs does *ForgotIt?* make? The encryption in *ForgotIt?* is highly secure by contemporary standards and has been developed with care and attention to detail on the basis of standard algorithms, but the main focus is data integrity. Version 2.0 or higher encrypts each database item individually, which is slow and slightly less secure than encrypting the whole file at once but drastically increases chances that the application may recover parts of the database when the file has been corrupted. Usability has also been a main development goal, since an encryption program that no one wants to use because it sucks would neither improve security nor sales.

Physical Security. Particularly people that (rightly) care about their privacy sometimes go to great lengths at securing their passphrases and other data by encryption programs and a corresponding 'ultra-secure' computer setup, yet they have a lock on their door that any amateur can open and their computer is not sealed against hardware tampering. This doesn't make much sense. If you're really that paranoid you need a really good lock on the door, surveillance equipment or at least should seal your computer case with tamper-proof paper seals like they are e.g. used by customs and police. In many cases this will not be worth the effort, though.

Software Security. Here is some general advice: Always apply the latest security updates of your operating system. Run anti-virus software regularly and use one from a reliable vendor. Lock your screen when you leave your computer unattended. Do not generally use an administrator account. Use Firefox instead of Safari or Internet Explorer. Do not install or run software from sources you don't consider fully trustworthy. Do not click on email links and always open SSL encrypted websites (such as those of banks) by typing their address directly into the browser's URL window. If you find a USB stick with write protection, switch write protection on when transferring data such as PDFs or PowerPoint presentations from the stick to an insecure machine. (Unfortunately, such USB sticks become rarer and rarer.) When surfing to shady web sites or running Adobe Flash movies or 'applications', it might also be a good idea to configure a browser to work in a secure sandbox mode or run the browser on a virtual machine. Never log into a site under an unencrypted http connection when browsing on a public WIFI net. Encrypt your wireless network at least with WPA2 (WEP is totally insecure, WAP is also broken). If you take all of these advices seriously your computer should remain fairly secure.

Note: *Although convenient and sometimes even unavoidable, storing confidential data in the clipboard must be considered insecure. ForgotIt?2.5 and higher attempts to delete confidential information from the clipboard when the application quits, but this method is not reliable because the operating system does not make the necessary security guarantees.*

How Much Security do You Want? It doesn't make much sense to protect information with encryption technology when at the same time anybody can easily infer it from your Facebook pages. If you care about privacy, don't give away your personal data to Google, Facebook or 'the cloud.' These companies do not make billions of dollars every year by providing free services to everyone, they make money by selling data to advertising companies or are advertising companies themselves. You are not their customer, you are their product.

4.2 Choosing a Good Passphrase

There are different types of passphrases and different ways to obtain a good passphrase. There is also plenty of information on the Web about passphrases. What makes a good passphrase? That depends on a variety of factors: What it is intended for? What restrictions are there (some websites have a maximum length)? How important is the corresponding site/access privilege/information to you? (i.e. How bad would it be if someone stole it?) Here are some rules of thumb that I personally find useful and reasonable:

A good passphrase must be hard to guess by the adversary but should be easy enough to remember by you. This is obvious. Assume that your adversary knows a lot about you—your mother's name, your birthday, your partner's name, phone number, etc. Also: Do not use PIN codes from credit cards.

A good passphrase must be at least 12 characters long. A passphrase must be easy to remember *and* must not have less than 12 characters. In fact, it should have 16 characters or more. The reason for this is that the entropy, a measure of 'randomness', of whatever can be typed on a keyboard and humans tend to come up with is surprisingly low. In other words, even if you think what you type is totally random it will not be random at all. For very high security a 32 character passphrase can be fairly reasonable. However, you still have to be able to remember it or need to have a secure place where to keep it.

Use a passphrase instead of a password. Single passwords are only secure as long as they have at least 8 characters and are generated randomly. Even if they contain pronounceable words or syllables, which have low entropy, passphrases consisting of many words are generally more secure than mere passwords. Of course, it is a good idea to use nonsensical phrases, vary punctuation (e.g. exchange space for another letter), vary capitalization (within words), and add special characters. It is relatively safe to use a personal 'obfuscation' scheme as long as you keep this scheme strictly secret. If on the other hand an 'adversary' finds out the way you build your passphrases, their security will be reduced significantly. Sometimes people think

they are really ingenious and can use relatively short passwords, because nobody else will find out the great way in which they add numbers. Most of the time, they are wrong. (Even a home/hobbyist hacker can build a terrabyte-sized dictionary nowadays.)

Use special symbols, upper- and downcase characters, and numbers in the passphrase. Just by adding uppercase characters the security of a passphrase can be significantly enhanced.

Never reuse a passphrase. Reusing a passphrase gives an 'adversary' instant access to other sites or machines, which also opens numerous new attack vectors. Sometimes people think: "'X' is so unrelated to 'Y', nobody would every try my X password at Y." That's not a good idea. Trying the same passphrase at different sites is among the first things an 'adversary' would do.

The quality of the passphrase must match the importance of the data. Spent your efforts on securing the really important data. You should pay particular attention to choosing very long and secure passphrases for sites that store your credit card information. If it is possible at all, you should avoid storing credit card information on web sites altogether. No store needs to keep your credit card information longer than it takes to process it, and usually the store doesn't even need to be able to see the information then, since the processing is done by a reliable 'payment service provider.' Speaking of which: Avoid payment providers, stores, or virtual banks that are in reality not banks at all (some people have criticized Paypal for this), especially if they try to convince you that it is better to store your credit card information or, even worse, continue to store it after you have deleted your account.

Do not use trivial passphrases that can be found in dictionaries. The previous advice ought not be taken to mean that it is okay to choose totally trivial passphrases for unimportant sites. Make *all* passphrases long enough and hard to guess, just take *extra* care with the most important ones. Never use any kind of keyboard pattern, no matter how ingenious you think it is, and never use any simple combination of a word with some numbers.

All keyboard patterns, all combinations of word+number, word+special character+word, number+word, etc. are in dictionaries. Reversed variants or spelling variants are in dictionaries. Wherever your family comes from, all words of your native mother tongue (or your parent's mother tongue) are in dictionaries. All short palindromes and simple anagrams are in dictionaries. Even the dictionaries used by hobby hackers are *huge* nowadays—it is entirely possible and in fact a hobby of many password crackers to compile a dictionary of a terrabyte in size or larger. Hence, only a combination of several words/syllables, special characters, and digits will do.

4.3 *ForgotIt?*'s Encryption

In this section, *ForgotIt?*'s encryption scheme is explained in detail. In future versions, this scheme might be updated to provide higher security margins, which in turn means that files will be saved in a new format that older versions cannot read. If a file is encrypted with an encryption scheme that the application cannot read, an error dialog will report this and indicate the version required to decrypt the file.

Master Key Schedule. The passphrase is a UTF-8 string. This string is concatenated with itself 32 times and the result is concatenated with a 16 bytes long random salt obtained from the operating system's default pseudo-random number generator. The result of this operation is hashed with SHA-256. The resulting intermediate key is concatenated with itself and then hashed again with SHA-256, a process which is repeated 32 times in total. The result is the master key.

Subkey Derivation. The master key is hashed using RIPEMD-160 and the first 8 bytes of the result of this operation are used as a seed for a (cryptographically insecure) linear-congruential random number generator. 120 bytes of output from this generator are then encrypted with Camellia-256 on the basis of the master key and a random initialization vector. The result is divided into the 3 subkeys: a 448 bit Blowfish key, a 256 bit AES-256 key, and a 256 bit Camellia-256 key.

Encryption. Pass 1: 32 bytes of pseudo-random data are concatenated with a SHA-256 hash of the plaintext and the plaintext. The Blowfish subkey and a random initialization vector is used to encrypt the result of this operation. The concatenation of the random initialization vector with the result of the encryption is the result of pass 1. Pass 2: Like pass 1, except that the input is the result of pass 1 and the AES-256 and is used with the AES subkey. Pass 3: Like pass 2, except that the input is the result of pass 2 and the Camellia-256 cipher is used with the Camellia subkey. The final result is Base64 encoded.

Decryption. For decryption, the whole process is reversed.

Regarding the initial key stretching described in the Master Key Schedule it should be noted that many standard key stretching algorithms hash the passphrase much more often to prevent attacks based on Rainbow tables—1000 or more iterations of SHA2 are common. Unfortunately performance of such key stretching algorithms on older machines turned out to be too slow and so the given schedule was chosen as a trade-off. In combination with the partially keyed subkey derivation I believe the current method to be reasonably secure.

5 Command Reference

5.1 The ForgotIt2 Menu (OS X only)

About ForgotIt... Display information about *ForgotIt?* and about the license. When the applications is not yet unlocked, this dialog allows you to buy the program at a secure webpage and enter your registration code afterward.

Preferences Cmd , Display a preferences dialog that allows you to adjust the global settings of the application. See section 3.5 for more information.

Services Access to the standard system-wide services section.

Hide ForgotIt2 A standard menu item that hides *ForgotIt?*.

Hide Others A standard menu item that hides all other applications and such that only *ForgotIt?* windows remain visible.

Show All A standard menu item that shows all previously hidden applications.

Quit ForgotIt2 Cmd Q Quit the application. You will be asked to save changes if unsaved changes to open documents have been made.

5.2 The File Menu

New Cmd Shift N Create a new, untitled *ForgotIt?* document.

Open Cmd O Open an existing *ForgotIt?* document. *ForgotIt?* can open UTF-8 encoded XML that have been saved by *ForgotIt?*. These files have the suffix '.forgotit' Old legacy files of *ForgotIt?* 1.4 or lower cannot be read directly by version 2.0. They need to be imported from an unencrypted *ForgotIt?* 1.4 XML file. To do this safely follow the instructions given by the *Import Wizard*.

Close Cmd W Close the frontmost document, asking you to save changes before closing if any unsaved changes have been made.

Save Cmd S Save the frontmost document. If you save a document the first time, you will be prompted to select a filename and choose a location to save to. If you have opened an existing document, it will be saved to the previous location without prompting for a file name. If no encryption passphrase is set yet for the document, you will be prompted to enter one before the document is saved.

Save As... Cmd Shift S Save the frontmost window under a new name. You will be prompted to enter a new name and a location to save to. After the file has been saved, the document will have the new name and future changes are saved to the new location.

Import → ForgotIt? 1.4 Import Wizard... (OS X only) Cmd Shift O Open an *Import Wizard* dialog that guides you to the process of migrating from an old *ForgotIt?* 1.4 database file to the new format. This menu entry is only available on OS X, because it requires an old copy of *ForgotIt?* 1.4 to run on the same machine, which only runs on OS X versions 10.3 to 10.6.

Import → ForgotIt? 1.4 Plaintext XML... Cmd Alt O Import an existing plaintext XML database that has been saved in *ForgotIt?* 1.4 using the program's *Extended Export...* option that is available in *ForgotIt?* 1.4 by pressing Alt while selecting the *File* menu.

Export → Plaintext as XML... Cmd Alt S Export the current document in unencrypted form as an XML file of *ForgotIt?* version 2.0 or higher. Exporting a database in unencrypted form is insecure and not recommended. This file format can be read by *ForgotIt?* version 2.0 or higher.

Export → Plaintext as PDF... Cmd Alt P Export the current document in unencrypted form as a PDF file. Exporting a database in unencrypted form is insecure and not recommended. This file format cannot be read directly by *ForgotIt?*.

Page Setup... Cmd Shift P Setup the page layout for printing and choose various printing options like the format of the paper to use (A4, letter, etc.).

Print... Cmd P Opens a platform- and printer-specific dialog that allows to adjust various settings related to printing and to print the document as a whole. Printing is insecure, because it invariably leaks plaintext to disk.

5.3 The Edit Menu

Undo Cmd Z Undo the last changes that have been made to the frontmost document. *ForgotIt?* supports as many undo and redo operations as main memory allows. Notice that most but not all actions can be undone.

Redo Cmd Y Redo the last change that was reverted by the *Undo* command. Every command that has been undone can be redone again.

Cut Cmd X Cut out the current selection in the current edit field or in the main list and put it into the clipboard.

Copy Cmd C Copy the current selection of the current edit field or main list to the clipboard. Text in an edit dialog or other edit fields is copied as plaintext. Items in the main list view of a document are copied as text to the clipboard in encrypted form that can only be decrypted by the same running version of *ForgotIt?*. It is not possible to copy items from the main list and paste them into another running version of *ForgotIt?* or quitting the application and pasting them into the a freshly started copy, because the temporary key is only held at runtime and immediately discarded once it is no longer needed.

Paste Cmd V Paste the current clipboard content into the current edit field or into the main list. Notice that main list entries can only be pasted into the main list and text entries can only be pasted into an open edit dialog. If a previously copied selection of the main list view is of another category than the currently selected category, the appropriate category is activated first. If items copied to the clipboard belong to a category that has the same name as a category in the current document but the categories differ in other ways, then an appropriate new category (with a number attached to the name) will be created in the document before the items are added to it. There is currently no way to copy & paste items between different categories. This shortcoming will be addressed in future versions.

Clear Cmd Shift X The currently selected text or the currently selected items in a main list view are deleted.

Select All Cmd A All items in the main list or all text in the currently active edit field of an edit dialog are selected.

Find Entry Cmd F Moves the input focus to the *search field* in the top right area of the currently active main document window. To search for an entry in the current category, simply enter one or more search terms into the search field. To clear the selection of documents that have been found, delete all characters in the search field.

New Entry Cmd N Create a new item of the currently selected category, opening an edit dialog where you can enter the data of the new item. When you have accidentally created a new item and wish to cancel the action, you may close the freshly opened edit dialog immediately without making any changes to it.

View Entry Cmd E View or edit the entry or list of entries currently selected in the main list view. This is the same action as pressing Enter when the main list view has the keyboard focus. See section 3.3 on page 12 for more information.

Set Passphrase... Cmd K Set or change the passphrase for the currently frontmost document. See section 3.3.1 on page 14 for more information.

Edit Categories... Cmd Alt K Open the *Category Window* where the document's categories can be changed and new categories can be added. See section 3.4 on page 15 for more information.

Preferences... (Linux and Windows only) Cmd , Open the *Preferences Dialog* where global application settings can be adjusted. See section 3.5 on page 19 for more information. On OS X the preferences menu item is under the *ForgotIt2* menu described above.

5.4 The Windows Menu

Clipboard Window Cmd B Toggle display of a small window that displays the current content of the clipboard.

Log Window Cmd H Open the *Log Window* that displays a history of recent security-relevant actions and possible errors that have occurred. See 3.6 on page 23 for more information.

Show Main List Cmd M When an edit dialog is active, show the corresponding main document to which the item being edited belongs. If another category than the one the item belongs to is currently active in the main list view, the view will be automatically changed to display the item's category..

Next Category Cmd → on OS X, Cmd] on Windows and Linux. Switch to the next category in the main list view (according to the defined order, which may be changed in the document's *Category Window*).

Previous Category Cmd ← on OS X, Cmd [on Windows and Linux. Switch to the previous category in the main list view (according to the defined order, which may be changed in the document's *Category Window*).

5.5 The Help Menu

View the User Manual as PDF Cmd Shift ? Open this manual in the system's preferred PDF viewer.

Buy ForgotIt? Online... (if not yet unregistered) Open the system's default web browser and visit the online shop, where you may buy the full application. Credit card and payment processing is provided by *Fastspring*: `http://www.fastspringstore.com/` – a well-reputed and secure online payment processing company. All transactions are SSL encrypted.

Go to the ForgotIt? Website... Open the system's default web browser and visit the homepage of *ForgotIt?*, where you can buy the application and download new versions of it.

Check for New Version of ForgotIt?... Checks online whether a new version of *ForgotIt?* has been released. You may also enable or disable automatic version checking in the preferences dialog.

About *ForgotIt?*... (Linux and Windows only) Open the *About Dialog* which displays version information. If the application is not yet registered, you may enter your registration code and unlock the application in the About Dialog. The full version number of the application is displayed in small letters in the top right corner of the dialog. Under OS X, the About menu item is located under the standard *ForgotIt2* menu.

6 Registering and Unlocking *ForgotIt?*

ForgotIt? is shareware. You may try the application for 14 days. If you continue to use the application on OS X or Windows after the trial period, you need to buy a license key. You can buy the application on the Web at the following address:

```
http://peppermind.com
```

The *Peppermind* Store supports all major credit cards, checks, and money transfer. After buying you will receive an email containing your license key. Please keep this email and the license key in a safe place for future reference. You may also add the license key as a serial number into a *ForgotIt?* database.

To unlock your copy of *ForgotIt?*, open the *About Dialog* (*Help : ForgotIt?...* or *ForgotIt2 : About ForgotIt2...* on OS X) and press the *Unlock Application* button. In the dialog that shows up, enter your name and optionally the name of your company. This data cannot be easily corrected later, so please make sure you spell everything correctly. (Nobody will keep you from calling yourself Duffy Duck in this dialog but please don't complain when you then see this name in the About box every time you open it.) In the Registration Key field, please enter the key that was sent to you exactly as it was sent to you (minus any surrounding spaces or newline characters).

Pressing the *Unlock* button will personalize the application to you and remove the shareware reminder. If you have any troubles unlocking your application, please contact `support@peppermind.com` for help.

ForgotIt?'s registration is based on user accounts. If you make a new user account on the same machine, you may need to enter the registration key and unlock the application again. Likewise, the application needs to be unlocked again when you upgrade to a new machine. You may also unlock copies on several machines, *as long as these are solely used by you and no-one else.* Please do not share your license code with anyone, publish it, or give it away. For more information, please read the license in Appendix I.

Shareware means low-price, high quality software that anyone can try before buying it. By buying a license you support future versions, the development of other useful applications, and hobby developers or small businesses who care for their customers!

7 Contact

ForgotIt? is distributed by *Peppermind.com*, a small software company that was established in 1997. Check out `http://peppermind.com` for more details and other cool software.

Please send your question, comments, bug reports, or feature requests to `support@peppermind.com` and we will reply as soon as possible!

Appendix

7.1 I. License

Shareware Fee. You, the licensee and end user of *ForgotIt?*, have to pay the shareware fee if you continue to use the Windows or OS X version of *ForgotIt?* after a trial period of 14 days. You may not share or give away the key.

Protection of Privacy. You may not decompile or otherwise analyze *ForgotIt?* except for the sake of security auditing whose result is published in a freely accessible form to the whole world. You may not create fake versions, faksimiles, or use other means to create an experience closely resembling that of using *ForgotIt?* for the purpose of obtaining access to a user database without prior voluntary consent by that user. You may not attempt to gain access to a *ForgotIt?* database of another user without prior voluntary authorization by that user. It is your responsibility to ensure prior to using the application that the use of strong encryption software is legal in your country and the intended use conforms to the laws and regulations of your country and workplace.

Security Statement. *ForgotIt?* has been developed with care and security in mind. The software contains no known backdoors and its developers and distributors do not believe it is possible to decrypt an encrypted *ForgotIt?* database without full knowledge of the passphrase that was used for its encryption. *Peppermind.com* does not assist in any attempts to decrypt *ForgotIt?* databases.

Limitation of Warrantability. Even with the greatest care it is not possible and not realistic to create a software program that is 100% free of errors or bugs. The software is provided 'as is' and the user has been given adequate time to test whether it suits her/his purposes. Therefore, neither the creators of *ForgotIt?* nor the distributor *Peppermind.com* can be held responsible in any way for any perceived or real damage or legal matters that result from the use of *ForgotIt?*.

7.2 II. Thanks and Attributions

Many thanks to all developers of the *Racket* programming language and Matthew Flatt in particular. Also many thanks go to the package contributors Dimitris Vyzovitis, Hans Oesterholt-Dijkema, and all other contributors to the Planet library. Many thanks to all the users of the *Racket* mailing list for useful help and advice. Many thanks also go to Andrew Barry, Art Makreel, and all our beta testers for their bug reports, as well as all of my users and customers who have given met valuable feedback over the years.

More thanks: Many thanks to P. J. Onori (aka somerandomdude) for having made available his 'iconic' icon set under the Creative Commons Attribution Share Alike 3.0 License. Some of his icons are used in the application. Thanks to '3dlb' for having made available his lock icon for free. And finally, many thanks to Teekatas Suwannakrua, a professional book illustrator based in Thailand with a very unique style who made another nice icon available under the Creative Commons Attribution License.