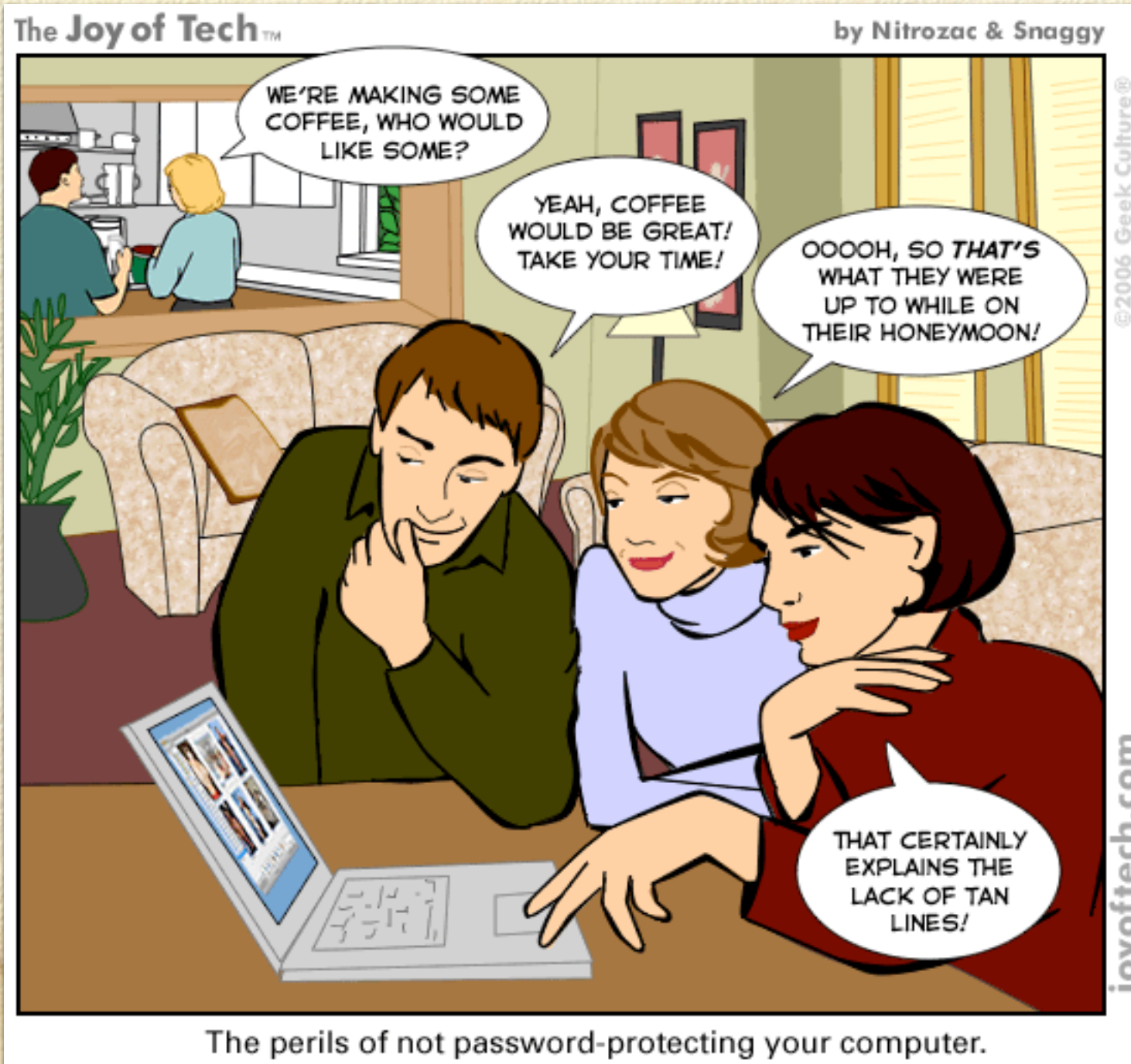




# What, me worry?





# Passwords

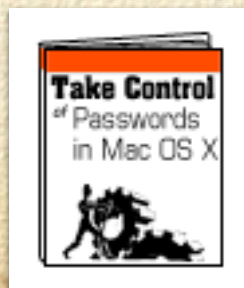
---

*Mac OS X passwords*

*Keychain*

*Password managers*

*Auto-fill Forms*



“Take Control of Passwords” ebook from  
[www.takecontrolbooks.com](http://www.takecontrolbooks.com) \$10  
10% discount on all books using CPN31208MUG



# Why Passwords?

---

- ❑ Identity: So a web site knows you
- ❑ Security: To lock sensitive information
- ❑ They can be stored in:
  - ❑ Apple's keychain
  - ❑ 3rd party password managers
  - ❑ Password database of many web browsers



Online Banking

member number:

password:



# What's your Risk?

and what do you have to lose?

Security	Simplicity
High crime area	Low crime area
Sensitive financial, personal & business info	No sensitive info
Laptop	Desktop
In hotels, airports	At home
Shared with students or coworkers	Only trusted family



# The Simple Life

---


- ❑ NO personal or sensitive info or email  
Nothing to hide
- ❑ Use automatic login
- ❑ Use a blank password when possible;  
otherwise use the same, simple password
  - ❑ Tape it to your computer
- ❑ Keep your Mac home; no one else uses it
- ❑ NO file sharing or wireless



# Default Installation

---

When you get a new Mac

- ❑ One Administrator account.   
Long name, short name & password
- ❑ Auto login is enabled.  
Some may forget they have a password
- ❑ Keychain password is the same as login
- ❑ Default is OK for a low-risk user.  
High-risk users should change it



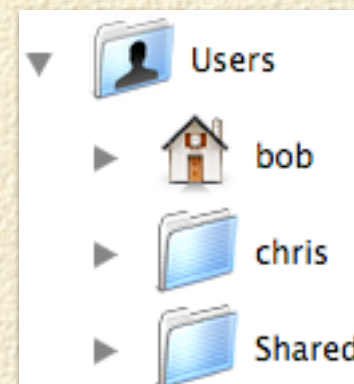
# User Accounts - You can have several

---

- Default installation: one administrator account.  
Admin can install apps & change the System

- Add accounts for other users  
Keeps their stuff separate

☒ Allow user to administer this computer



A second account  
is useful for  
troubleshooting

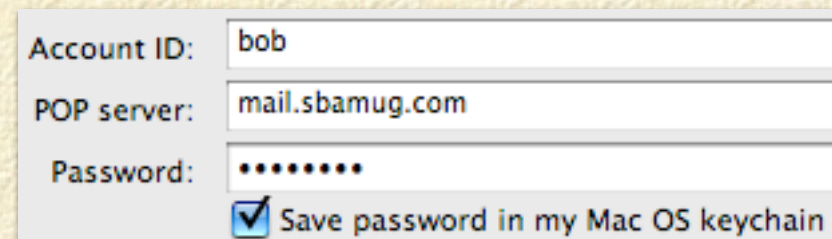
- Each account has its own private space with a name and password.
- Manage accounts in System Preferences



# Keychain stores passwords

---

- A system wide repository for passwords



A screenshot of a Mac OS login dialog box. It contains three text input fields: 'Account ID:' with the value 'bob', 'POP server:' with the value 'mail.sbamug.com', and 'Password:' with a masked password represented by eight dots. Below these fields is a checkbox labeled 'Save password in my Mac OS keychain', which is checked.

- A keychain is created for each user account
  - **Default password is the login password.**
  - Unlocked automatically - not very secure
  - Change it with “Keychain Access”



# Keychain Limitations

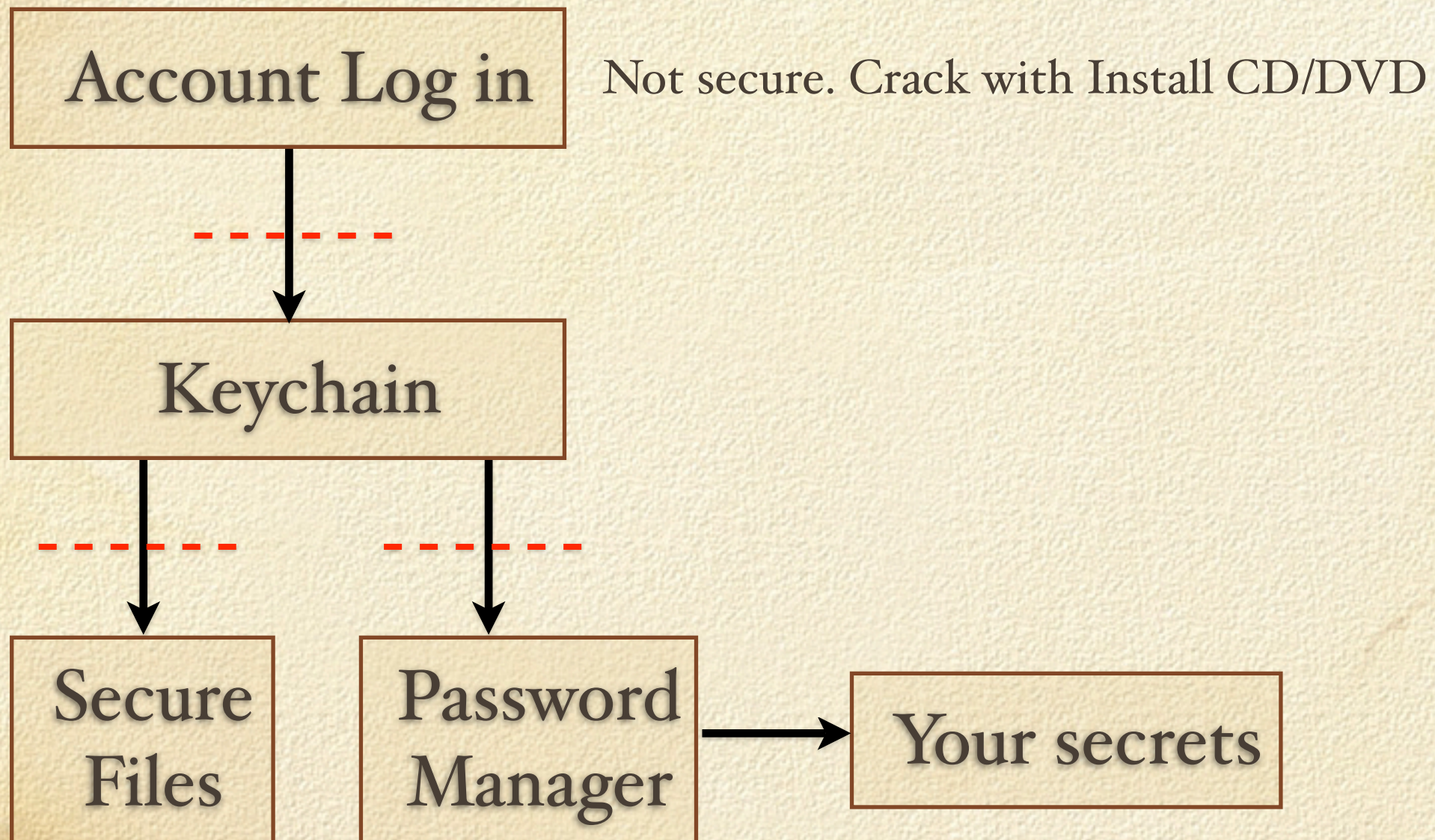
---

- ❑ Not all applications support it
- ❑ Some web sites thwart autofill
- ❑ Not as secure as other methods, but still pretty strong
- ❑ Lots of 3rd-party password managers



# The Weakest Link

---





# Passwords - How strong?

---

## Simplicity versus security

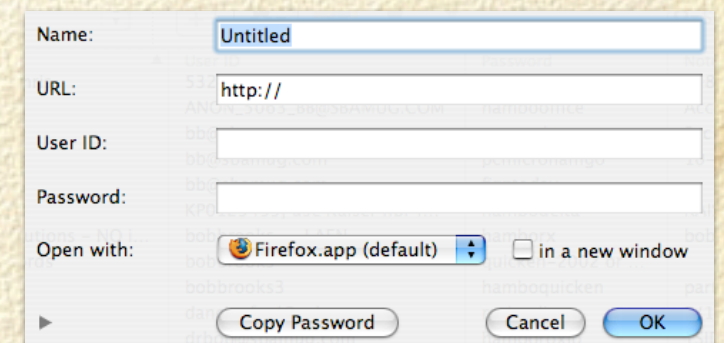
- ❑ Benign uses: Use a simple password
- ❑ High risk requires strong passwords.
  - ❑ Strong: Ed552C%^”Bn
  - Medium: npspfrcr
  - Easy: fido
- ❑ Hard to remember? Use a password manager
- ❑ Passphrase: Easy, yet secure  
SBAMUGmeetingeverylastwedsinRB



# Password Manager: a special database

- Use a strong master password (phrase) to open
  - May auto-lock after a set period
- Organize passwords by category
- Stores URL, ID, password and notes
- Click or auto-paste URL, ID & password
- Export to text, dot mac, iPods, Palm etc.
- Find box 

I have over 200 items in Web Confidential
- Creates secure passwords



A screenshot of a password manager dialog box. It contains the following fields and controls:

- Name:** A text field containing "Untitled".
- URL:** A text field containing "http://".
- User ID:** An empty text field.
- Password:** An empty text field.
- Open with:** A dropdown menu showing "Firefox.app (default)" and a checkbox labeled "in a new window".
- Buttons:** "Copy Password", "Cancel", and "OK".



# Password Managers

---

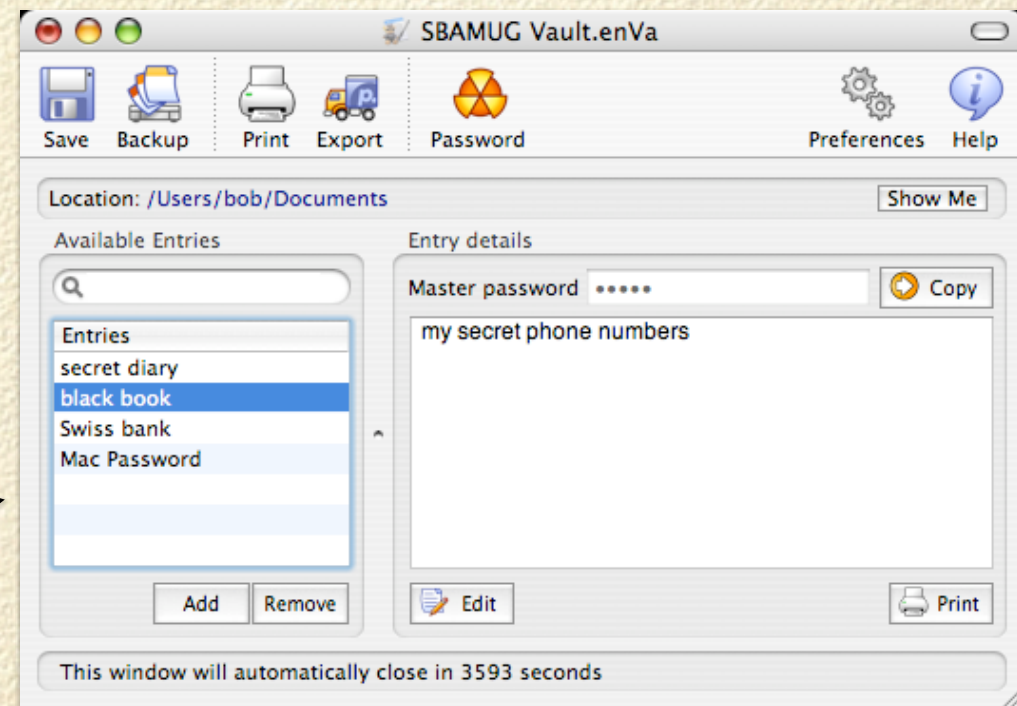
❑ Web Confidential, \$20

❑ iPasswrd, \$30

❑ PasswordVault, \$15

❑ Password Wallet, \$18

❑ Vault is free



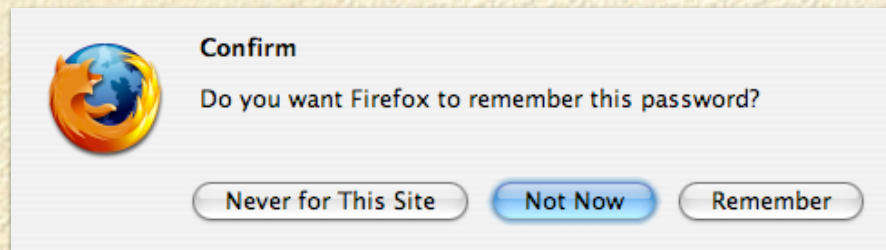
❑ Yojimbo, \$39, but it's much more than a PM



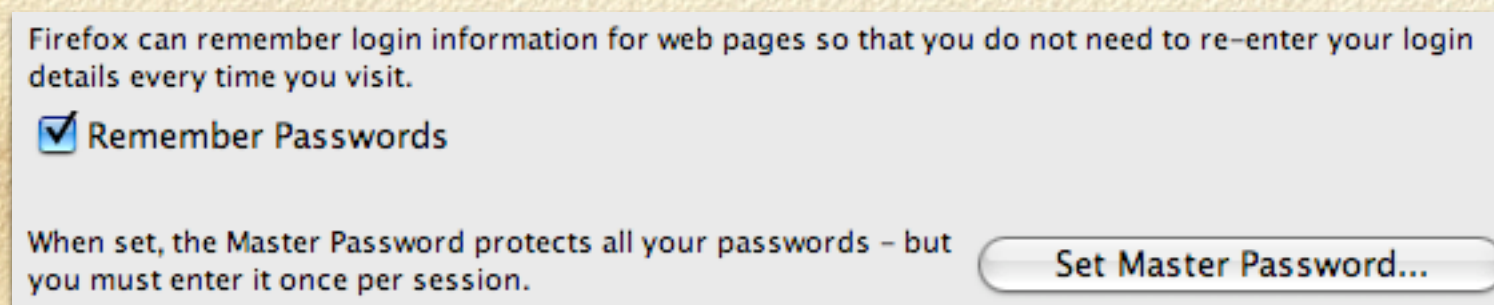
# Autofill Forms & Passwords

---

- ❑ Some browsers automatically insert personal information. Safari uses Address Book.
- ❑ Some browser (e.g. FireFox) save passwords.




- ❑ Master password option.





# Secure your Files

---

- ❑ See August 2006 newsletter for “how to do it”
- ❑ Put the files in a folder
- ❑ Create an encrypted disk image 
- ❑ Put (copy) files inside and delete originals



# Backup

---

- ❑ Back up your password files.  
Keychain: library>keychains  
user>library>keychains
- ❑ Keep your master passwords in a safe deposit box or with a loved one. Make sure they know how to use it.
- ❑ Write it on page (birth) of favorite book, or  
1 tbsp s8#gU14Bx5; 3 tbsp ground pepper

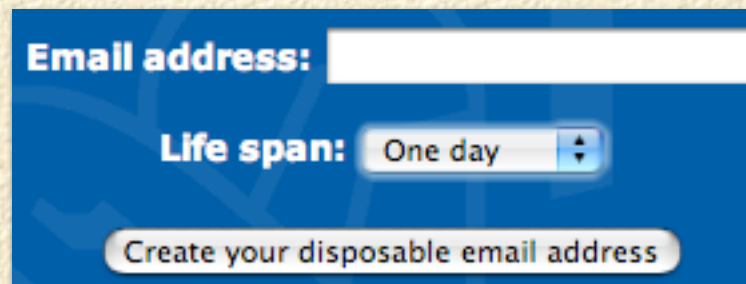


# Protect your Email address

---

A little off the topic

- ❑ Hundreds of sites want your email address
- ❑ Worried about spam?  
Use disposable addresses. [www.jetable.org](http://www.jetable.org)



The image shows a blue rectangular interface for creating a disposable email address. It features a white text input field for the email address, a dropdown menu for the lifespan (currently set to 'One day'), and a button labeled 'Create your disposable email address'.

Email address:

Life span: One day

Create your disposable email address