

CHAPTER 3

User Authentication

49

INTRODUCTION

When web applications enable one-to-one interaction and store user-specific information, they require users to create an account (REGISTRATION) and choose unique credentials to access the web applications. Registering may require users to enter a set of alphanumeric characters from a distorted image to prevent spam and ensure that registering users are human and not automated computer programs (*CAPTCHA*, Completely Automated Public Turing test to tell Computers and Humans Apart).

Once unique credentials are established, users can identify themselves (LOG IN) and store and access their personal information. After logging in and accomplishing desired tasks, users often need a way to exit the application to ensure that unauthorized users cannot access and modify their account information (LOG OUT). Many applications also have provisions for automatically logging out users after a certain period of inactivity (AUTOMATIC LOGOUT).

Because many web applications are used occasionally, users often forget their login information and need a way to retrieve it. Depending on the security level of the applications, users may be asked to provide one or more pieces of unique information about their account. It can be as simple as providing the email address associated with the account or answering one or more security questions that were established during registration (FORGOT USERNAME/PASSWORD).

REGISTRATION

Problem

Web applications often need to uniquely identify users. The reasons include preventing unauthorized access to personal and sensitive information (e.g., financial or health records), increasing convenience (e.g., storing billing and shipping addresses), and enabling sharing (e.g., photos). Despite such benefits, users often hesitate when providing personal information and often shy away from applications that require them to set up an account.

Choose a plan that fits your needs

Plans can be changed at any time, so feel free to start using Crazy Egg with a free plan.

The screenshot displays the Crazy Egg registration interface. On the left, a table lists features for different plans. The 'Basic' plan, priced at \$9/month, is highlighted in green and offers 10,000 visits, 10 pages tracked, advanced features, and live reporting. To the right, a registration form titled 'Grab an account now' includes fields for email, password, and a re-type password. Below these fields is a checkbox for agreeing to the terms of use and privacy policy, and two buttons: 'CANCEL' and 'SUBMIT'.

	Basic \$9 / month
Visits you can track per month	10,000
Pages you can track at once	10
Advanced Features	✓
Live Reporting	✓

Grab an account now

Email:

Password: Re-type password:

☐ I have read and agree to the [Terms of Use](#) and the [Privacy Policy](#).

FIGURE 3.1

Crazy Egg has one of the shortest and simplest registration forms. To register, users only need to provide their email address and password and agree to the terms of use and privacy policy.

Solution

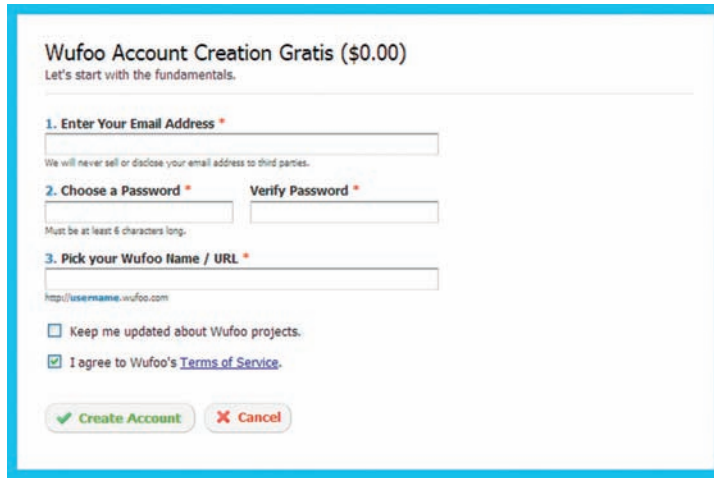
Delay registration for as long as possible and allow users to explore the application so that they fully understand the benefits of setting up an account. In addition, if users are willing to forego some convenience, make it possible for them to transact without registering. Topix.net found a significant increase in the number of posts and a substantial improvement in their quality when they removed the registration requirement from their discussion forums (Blake, 2006). When registration unavoidable, clearly indicate the benefits of registration and ask users only for the information necessary to set up an account (Figure 3.1).

Why

For most applications, setting up an account or registering is not one of the users' goals. Their goals typically include purchasing an item, sharing information, paying bills, and so forth. Asking users to register is usually an interruption in their interaction experience, since it distracts them from their primary goals. Therefore, registration should be delayed as long as possible. This is common in e-commerce applications (e.g., Amazon, Buy.com), content portals (e.g., Yahoo!, MSN, Morningstar), and content-sharing applications (e.g., Flickr, YouTube, SlideShare), which allow users to explore content without a user account. Only when users want to make a purchase, add content, make comments, or customize an application's look and feel do these web applications require users to register. Thus, delaying registration also allows users to experience the application's benefits and better understand the need and value of setting up an account.

How

First and foremost, keep registration forms as short as possible and ask only for essential information (Figure 3.2). For most applications, this includes a unique username (or user ID or email address) and associated password.

The image shows a web form titled "Wufoo Account Creation Gratis (\$0.00)" with the subtitle "Let's start with the fundamentals." The form is divided into three numbered steps. Step 1, "1. Enter Your Email Address *", has a text input field and a note: "We will never sell or disclose your email address to third parties." Step 2, "2. Choose a Password *", includes a "Verify Password *" field and a note: "Must be at least 6 characters long." Step 3, "3. Pick your Wufoo Name / URL *", has a text input field with a placeholder "http://username.wufoo.com". Below the steps are two checkboxes: "Keep me updated about Wufoo projects." (unchecked) and "I agree to Wufoo's Terms of Service." (checked). At the bottom are two buttons: "Create Account" with a green checkmark icon and "Cancel" with a red X icon.**FIGURE 3.2**

Wufoo, an online form-builder application, uses a simple registration form that asks only for the essential information for creating an account.

Because users cannot see the password they entered, ask them to confirm the password by reentering it. In addition, if required for legal reasons, ask them to agree to the usage terms and conditions.

When users need to set up an account, it's important that forms are as short as possible and ask only for relevant information so that users are distracted only for a very short period of time and can continue to accomplish their goals. Asking for nonessential information increases the time it takes to register and increases the chances of user errors. This may cause a user to abandon registration or provide incorrect or nonsensical data.

When asking users for any personally sensitive information, such as birth date, gender, race, and so forth, clearly indicate why the information is needed and how it will be used (Figure 3.3).

CONSIDER USING AN EMAIL ADDRESS FOR A USERNAME

When registering, users are often required to choose a unique identifier for their account such as a username or email address. Email addresses are often a better choice because they are always unique and are easier to remember even when users have multiple email accounts. In addition, when users have to be reminded of their login credentials, it's easier to send the reminder information to their registered email address (see FORGOT USERNAME/PASSWORD pattern later in this chapter).

USE CAPTCHA TO ENSURE REGISTRATION BY HUMANS

An increasing number of automated web crawlers have made it difficult to distinguish them from legitimate human users. Use CAPTCHA as part of the registration form to minimize registration by such automated agents (Figure 3.4).

Carefully enter your phone number below so Papa John's can contact you regarding your order should the need arise.

*Phone: - -

Cell Phone: - -

☐ Send me special text message offers from Papa John's

*You must be 13 years or older to order from Papa John's Online. Please enter your age below.

*Birthday: Month Day Year

Submit ➔

FIGURE 3.3 Papa John's registration form justifies asking users to enter their birth dates by indicating that they must be 13 or older to place an online order.

[Nabble 1](#) [New! Nabble2](#) [Login](#) : [Register](#)

Register


E-mail:	<input type="text"/>	NOTE: You will receive a confirmation link in e-mail to complete the registration.
Password:	<input type="text"/>	NOTE: Nabble stores passwords. (?)
Verify Password:	<input type="text"/>	
Your User (Screen) Name:	<input type="text"/>	NOTE: This will be your screen name shown in your posts.
		
Change code image		
To verify your registration, enter the code shown in the picture above:	<input type="text"/>	NOTE Code letters are not case sensitive.
<input type="checkbox"/> I have read and agree to Nabble's Terms of Use .		
<input type="button" value="Register"/>		

FIGURE 3.4 Nabble asks users to respond to a CAPTCHA image when registering.

CAPTCHA requires users to type characters from a distorted image containing letters and/or numbers before they can register. The ability to correctly identify characters from the distorted image is used as sufficient evidence that the user is human and not an automated agent (see the CAPTCHA pattern next).

Although the use of CAPTCHA is becoming common, it is yet one more piece of information users have to provide and should be avoided, if possible.

Calbucci (2008) found that removing CAPTCHA from the registration form improved the conversion rate by 9.2 percent on Sampa (www.sampa.com).

CONSIDER THE “LAZY” REGISTRATION APPROACH

As mentioned, registration is often an interruption in users’ interaction experience. Therefore, delay registration as much as possible and allow users to explore the application before asking them to register. For instance, Morningstar asks users to register or log in only when they land on a page that requires them to provide sensitive information (e.g., creating an investment portfolio) or when they are accessing content reserved for paying customers.

To make the registration process as efficient as possible, even when it is delayed, an option is to use a “lazy” registration approach, which is collecting information about users using browser cookies as they interact with the application. As Mahemoff (2006) states:

As the user interacts with the application, the account accumulates data. In many cases, the data is explicitly contributed by the user, and it’s advisable to expose this kind of information so that the user can actually populate it. In this way, the initial profile may be seen as a structure with lots of holes. Some holes are eventually filled out automatically and others by the user himself. (p. 475)

By collecting information in the background, when users are presented with the registration form, some of the registration fields can be prepopulated, requiring users to verify collected information rather than enter it. For example, if a user signs up for an email newsletter, the application has the user’s email address, which it can prepopulate on the registration form.

CONSIDER ELIMINATING REGISTRATION

Offer users the option to have access without registering in applications where they may just want to complete transactions quickly. This is common in e-commerce applications, especially those that support gift registries, where users may just want to purchase a gift and leave the application (Figure 3.5). Users may be prompted to register at the end of the transaction (or checkout process) with clearly listed benefits for doing so (e.g., track the order).

CLEARLY INDICATE REGISTRATION BENEFITS

For web applications where it’s not possible to delay registration, clearly indicate registration benefits to users (Figure 3.6).

For many applications, listing benefits may not be sufficient, especially when registering is not free. In such instances, offer users the option to take a guided tour that explains the benefits of using the application and/or allow them to set up a free-trial account for a limited time period or with restricted functionality (Figure 3.7).

Office DEPOT.
Taking Care of Business

1 Login 2 Shipping, Billing, Payment 3 Order Complete

Checkout

Log in to access your account information

Need Help?

Customer Service
Call Customer Service
1-800-GO-DEPOT
(1-800-463-3768)
24 hours/day, 7 days/wk

Security/Privacy
Your information is safe with us.
We secure your info using SSL encryption.
Click [here](#) to view our

Existing Customers - Login

If you already have an account, sign in below.

Login Name:

Password:

[Forgot your login name/password?](#)

LOGIN AND CONTINUE

New Customers

You are not required to have an Office Depot account to shop with us. Click button below to proceed.

CONTINUE CHECKOUT

If you'd like to set up an account, we'll show you how at the end of the Checkout process.

FIGURE 3.5 Office Depot offers users the option to purchase without registering. It also allows users to defer the registration decision until later, indicating that they can set up an account at the end of the checkout process.

FIGURE 3.6

Netflix not only lists registration benefits but also indicates on the same page how Netflix works. It offers links to users who want to learn more about the free trial offer or about movie selection and goes a step further by offering a phone number for users to call in case they have any questions.

Sign up today and try Netflix for FREE!

Now - plans from only \$4.99 a month

- You'll get free shipping both ways
- Watch classics to new releases to TV series
- Cancel anytime
- Watch assorted movies, TV episodes, and more instantly on your PC at no additional charge

How Netflix Works:

- 1 Over 85,000 Titles**
Create your list of movies online
- 2 Free Delivery to your door in 1 Business Day**
We rush you DVDs from your list
- 3 NO LATE FEES**
Keep each movie as long as you want
- 4 Prepaid return envelopes**
Return a movie to get a new one from your list

Start here

Email Address
Example: Cindy@aol.com

Create a Password

Re-type Password
4-10 characters (case sensitive)

Enter Zip Code

Secure Server **Continue**

We value your privacy. Netflix will not sell or rent your email address to third parties.

Want to learn more?
[Click. That's all it takes.](#)
[Browse our selection of movies](#)
[Learn more about Netflix](#)

Questions?
Call 1-800-715-2130
24 hours a day

CONSIDER USING “UNIFIED REGISTRATION” SERVICES

Remembering login information for more than a few applications can be difficult for users and lead to practices that could compromise the security of their personal information (e.g., writing down login information or using very simple passwords). Even when security is not a concern, forgetting login information could result in unnecessary delays in accomplishing tasks. Therefore, if feasible, allow users to register using “unified registration” services such as OpenID or Windows CardSpace.

An OpenID is an open standard that allows users to create and use one set of username and password to log in to any OpenID-enabled web application; for more information, visit www.openid.net. Thus, enabling support for OpenID can

The screenshot shows the Basecamp website. At the top, there's a navigation bar with links: Home, Tour, Case Studies, Buzz, Forums, Help/FAQs, Pricing & Sign-up. The 37signals logo is in the top right. The main banner says 'Get projects done' in large black text. Below it, a yellow box contains the text 'OVER 1,000,000 PEOPLE SIGNED UP WORLDWIDE'. The main text reads: 'Basecamp is the smarter, easier, more elegant way to collaborate on your internal and client projects.' Below this is another yellow box with 'Sign up for free or Take a tour' and 'Signup in less than 30 seconds. Got an account? Log in.' A quote from Robert Hof of BusinessWeek is included: 'Basecamp is so simple you can't do anything wrong. It's addictively easy-to-use.' Logos for Business 2.0, Fast Company, The Wall Street Journal, and BusinessWeek are shown. A 'Read more reviews and buzz' link is at the bottom. On the right, a screenshot of the Basecamp interface is shown, featuring a 'Our Projects' section with a list of projects and a 'Your projects' sidebar. A red banner on the interface says 'HAVE A SUCCESSFUL OR'.

FIGURE 3.7 Basecamp (from 37Signals) offers users an application tour so they can explore its functionality and benefits. It also allows users to sign up for a free-trial account so they can experience the application firsthand. Although the free-trial account has restricted functionality it makes it possible for users to easily understand the benefits of having an account.

Join Ma.gnolia

There are two ways to join Ma.gnolia: with an email + screen name, or with OpenID. Enter information only for the type of sign up you want to do.

Regular Signup

Enter Your Email Address

Choose a Password

Choose a Screen Name

Confirm Your Password

☒ Notify me about messages within Ma.gnolia and Ma.gnolia news.

JOIN FREE

By creating an account you agree to Ma.gnolia's [Terms of Service](#) and [Privacy Policy](#).

OpenID Signup

http://

OpenID lets you safely sign in to different websites with a single password. [Learn more](#), and [get your own OpenID](#).

VERIFY MY OPENID

FIGURE 3.8

Ma.gnolia offers users a regular registration process where they choose their login credentials, as well as supports registration using OpenID.

either eliminate the need for registration or at least minimize the information required from users to set up an account (Figure 3.8). Because not all users can be expected to have OpenID accounts, supporting a normal registration process is still important.

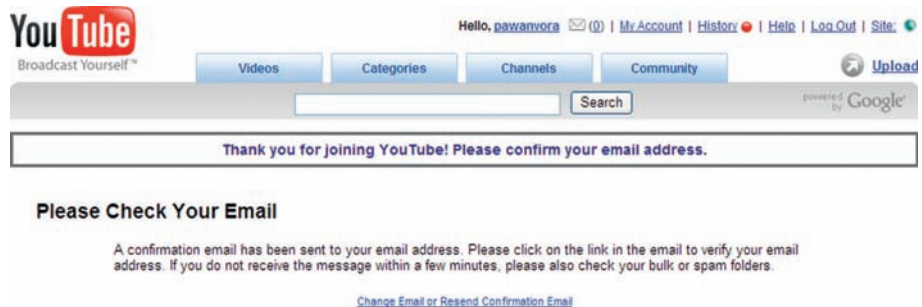


FIGURE 3.9 YouTube asks users to click the confirmation link in the email to complete their registration and then to check their spam folders if they don't see the message appear in their inbox within a few minutes.

FIGURE 3.10 Prosper provides a brief summary of their privacy policy on the registration form, as well as offers a link to a detailed privacy policy.

VERIFY REGISTRATION

If necessary, require users to verify their registration to prevent fraud and ensure legitimate user accounts. This is commonly accomplished by sending a message with a confirmation link to the email address provided by users during registration. Only after users have returned to the application by clicking the confirmation link (or by pasting the registration URL in their browser address field) do they consider their registration complete. To ensure email reaches users' email inboxes, ask them to check their spam folders (Figure 3.9).

ALLAY USERS' PRIVACY CONCERNS

Users may be hesitant to register because they may not know how their personal information will be used. Include a brief privacy statement (e.g., "Your information will not be sold or shared") followed by a link to a detailed privacy policy statement to address such concerns (Figure 3.10).

Update Security Questions (Step 1 of 2)
Note: You must select three questions and enter an answer for each question.

Security Question: What street did you live on in third grade? [v]
Answer: [text input] (1-32 characters, no special characters)

Security Question: What school did you attend for sixth grade? [v]
Answer: [text input] (1-32 characters, no special characters)

Security Question: In what town was your first job? [v]
Answer: [text input] (1-32 characters, no special characters)

Cancel Continue to Step 2

FIGURE 3.11 When setting up an account, CapitalOne requires users to set up security questions.

SET UP SECURITY QUESTIONS WHEN STORING SENSITIVE INFORMATION

Use security questions for web applications that require a higher level of security, such as for financial applications (Figure 3.11). Security questions can then be used to establish users' identities when they log in and/or when they need help retrieving their forgotten login information (see the FORGOT USERNAME/PASSWORD pattern later in this chapter).

OPT-IN

Ask users to opt in instead of opt out if the company supporting the web application plans to communicate with them in the future or send promotional information (Figure 3.12). This is the first step to making sure email sent to users is CAN-SPAM¹ compliant (Dixon, 2004; see also the Federal Trade Commission's SPAM home page at www.ftc.gov/spam/). The better practice is to use double opt-in, where upon opting in, users are sent an email confirmation with a link that they must click to finish the opt-in process.

In addition, set users' expectations by explaining how frequently they will receive communication and what kind of messages will be sent. With the possibility of email communication being stopped by spam filters, ask users to adjust their spam filter settings appropriately or add the "from email address" to their contact lists.

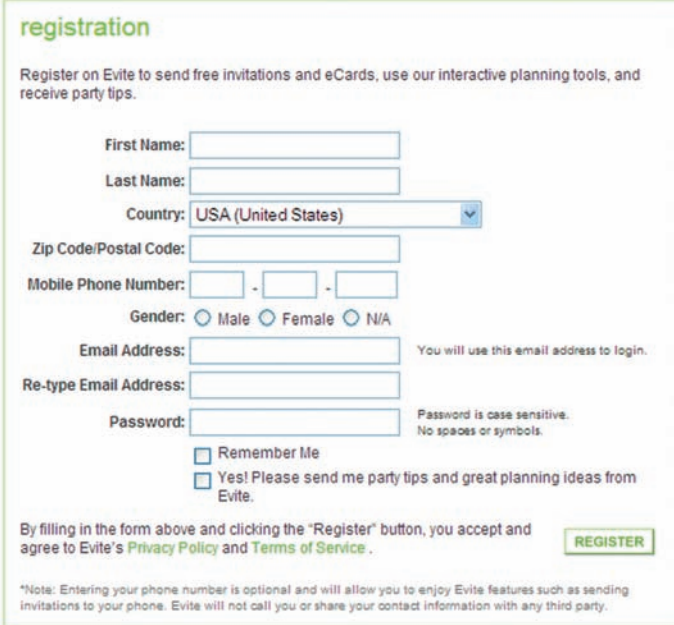
RETURN USERS TO THE NEXT LOGICAL STEP IN THE INTERACTION SEQUENCE

Upon the completion of registration, return users to the "page of departure"—that is, the page from where they chose to register or were required to register.

¹CAN-SPAM is a commonly used acronym for Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. It became a law on January 1, 2004, and applies to most businesses in the United States that send commercial email. It provides email recipients with the right to opt out (unsubscribe).

FIGURE 3.12

Evite offers users a clear opt-in option for sending party tips and planning ideas.



The image shows a web registration form titled "registration" in green. The form includes fields for First Name, Last Name, Country (a dropdown menu currently showing "USA (United States)"), Zip Code/Postal Code, Mobile Phone Number (with hyphens), Gender (radio buttons for Male, Female, and N/A), Email Address, Re-type Email Address, and Password. A checkbox for "Remember Me" and another for "Yes! Please send me party tips and great planning ideas from Evite." are located below the password field. To the right of the email field, a note says "You will use this email address to login." To the right of the password field, a note says "Password is case sensitive. No spaces or symbols." Below the form, a paragraph states: "By filling in the form above and clicking the 'Register' button, you accept and agree to Evite's [Privacy Policy](#) and [Terms of Service](#)." A green "REGISTER" button is to the right. At the bottom, a small note says: "*Note: Entering your phone number is optional and will allow you to enjoy Evite features such as sending invitations to your phone. Evite will not call you or share your contact information with any third party."

For example, in an e-commerce application, if users are asked to register at checkout, return them to the page they are likely to see if they were already registered or logged in, such as the shipping information page.

Related design patterns

For many web applications, registration may be the first form users encounter. To create a successful user experience, it's important to follow the patterns identified in Chapter 2—CLEAR BENEFITS, SHORT FORMS, REQUIRED FIELD INDICATORS, and ERROR MESSAGES. When presenting the registration form to users, it is important that they be given an option to LOG IN since they may have registered previously. In addition, because CAPTCHA often accompanies registration, follow the best practices identified in the following pattern.

CAPTCHA

Problem

The application needs to make sure that the action (e.g., register, provide feedback, send comment, and so forth) is initiated by a human rather than an automated agent to prevent creation of fraudulent accounts and fake responses.

Solution

Ask users to type characters from a distorted image that contains letters and/or numbers before they can register or provide comments or feedback (Figure 3.13).



FIGURE 3.13 CAPTCHA on Yahoo!’s registration page.

Decoding distorted images is used as a validation that a user is human and not an automated agent, since automatically decoding a distorted image is computationally intensive. This method is referred to as CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart (Ahn, Blum, and Langford, 2004).²

Why

An increasing number of automated crawlers on the Web have made it difficult to distinguish them from legitimate human users. By asking users to do something that is relatively easy for humans to do but difficult for automated crawlers, the use of CAPTCHA makes it difficult, if not impossible, for bots and crawlers to interact with the application and submit forms.

How

CAPTCHA images typically have about four to five distorted alphanumeric characters; the alphabetical characters in the image may include both uppercase and lowercase ones. In addition, they may have lines through them, more than one distorted word, noisy backgrounds, and so forth (Figure 3.14). Users are asked to decode the image and enter the alphanumeric characters in the correct order (they may or may not be case sensitive) before submitting the form. Upon form submission, the response is verified, and users are either taken to the next step or presented with an error.

Recently, some sites have included simple math problems in CAPTCHA images such as $2 + 4$ or 4×2 that users must answer (Figure 3.15).

ALLOW USERS TO CHANGE THE CAPTCHA IMAGE

Users may find some CAPTCHA images too distorted to distinguish between some characters (e.g., the number 1 versus a lowercase *l*, or the number 9 versus

²Many CAPTCHA images on the Web use the free CAPTCHA service offered by Carnegie Mellon University as part of their reCAPTCHA project, which helps digitize books by sending users digitized words as CAPTCHA that cannot be read by their OCR (optical character recognition) programs. For more information, visit www.recaptcha.net.



FIGURE 3.14 Examples of CAPTCHA images.

10 + 8 is equal to? (required)

9 3 + 8 =

FIGURE 3.15 Two examples of math CAPTCHA.

Register

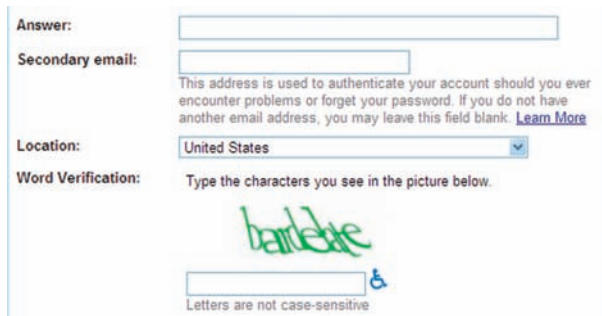
E-mail:	<input type="text"/>	NOTE: You will receive a confirmation link in e-mail to complete the registration.
Password:	<input type="password"/>	NOTE: Nabble stores passwords. (?)
Verify Password:	<input type="password"/>	
Your User (Screen) Name:	<input type="text"/>	NOTE: This will be your screen name shown in your posts.
		
Change code image		
To verify your registration, enter the code shown in the picture above: <input type="text"/>		NOTE: Code letters are not case sensitive
<input type="checkbox"/> I have read and agree to Nabble's Terms of Use .		
<input type="button" value="Register"/>		

FIGURE 3.16 Nabble offers users the option to change the CAPTCHA image.

a lowercase g). Therefore, users should be offered the option to change the CAPTCHA image by clicking on a “refresh” or “change” link (Figure 3.16).

OFFER AUDITORY CAPTCHA TO MAKE APPLICATIONS ACCESSIBLE

Because CAPTCHA is based on decoding the image, it presents an obvious obstacle for blind users or those with visual disabilities. They should be offered



The image shows a portion of a web registration form. It includes the following elements:

- Answer:** A text input field.
- Secondary email:** A text input field with a note below it: "This address is used to authenticate your account should you ever encounter problems or forget your password. If you do not have another email address, you may leave this field blank. [Learn More](#)".
- Location:** A dropdown menu currently showing "United States".
- Word Verification:** A section with the instruction "Type the characters you see in the picture below." followed by a CAPTCHA image showing the word "barbecue" in a green, stylized font. Below the image is a text input field and a small accessibility icon (a person in a wheelchair).
- Below the input field, it says "Letters are not case-sensitive".

FIGURE 3.17 Gmail offers both visual and auditory CAPTCHA.

a voice CAPTCHA—an audio version of CAPTCHA—that allows them to interact with the application (Figure 3.17).

Related design patterns

Use of CAPTCHA is common during registration, as most applications try to avoid fraudulent registrations by automated web crawlers (REGISTRATION). They are also common in discussion forums or blogs, where users can make comments or participate in communities (see the GROUPS/SPECIAL INTEREST COMMUNITY pattern in Chapter 9).

LOG IN

Problem

Users need to identify themselves so that they can access their account information and/or see customized or personalized versions of the web application. For example, users may want to check their emails (e.g., Hotmail, Yahoo! Mail), access their account to see the order status on an e-commerce application (e.g., Amazon, Dell), or see the customized version of their content portals (e.g., My Yahoo!, iGoogle).

Solution

Ask users to identify themselves by providing a combination of a unique identifier (e.g., username or email address) and password that they either chose when registering with the application or that was provided to them by the system administrator. Universal identity services that uniquely identify users, such as OpenID or Windows CardSpace, can be used as well to allow users to access a web application (Figure 3.18). In addition, to make it easy to access the application, consider offering users an option to let the application remember their login information.

Why

When a web application allows users to access their personal and/or sensitive information, it is important that users identify themselves by logging in with



Alpha Cube, Inc.

✓ Please log in first and then we'll send you right along.

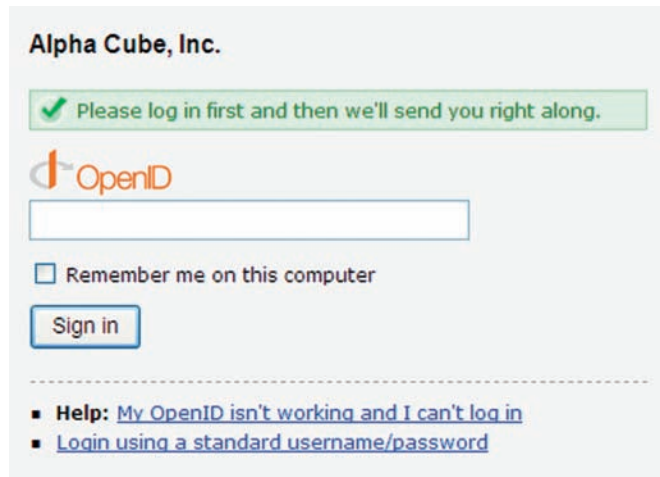
Username

Password

☐ Remember me on this computer


■ Help: [I forgot my username or password](#)
■ [Login using an OpenID instead](#)

(a)



Alpha Cube, Inc.

✓ Please log in first and then we'll send you right along.



☐ Remember me on this computer

■ Help: [My OpenID isn't working and I can't log in](#)
■ [Login using a standard username/password](#)

(b)

FIGURE 3.18 Basecamp allows users to log in using the username and password they chose during registration (a) or with their OpenID (b). Users may also choose to let the application remember their login information.

a unique set of credentials that they established while registering with the application. While logging in is an important task to secure account information and avoid unauthorized access, users may consider it an obstacle to accomplishing their goals. In addition, for applications not visited frequently, users may forget their login credentials and may be locked out for some time period. Therefore, where feasible, users should be offered the option to let the

Sign In

What is your e-mail address?

My e-mail address is

Do you have an Amazon.com password?

☐ No, I am a new customer.

☒ Yes, I have a password:

Sign in using our secure server

[Forgot your password? Click here](#)

[Has your e-mail address changed since your last order?](#)

FIGURE 3.19 Amazon lets users know they are logging in using their secure server.

application remember their login information. Offering users a “remember me” option eliminates the need to log in and makes it easier for them to accomplish their goals without unnecessary interruptions.

How

Require users to log in using their username or email and the password they provided during registration. However, like registration, logging in is an interruption to a user’s interaction experience. Therefore, delay it as much as possible. When logging in cannot be delayed for business reasons—for example, users must log in to select their delivery or pick-up store for ordering from food chains such as Domino’s or Pizza Hut for franchise obligations—consider alternative means for getting users closer to their goal—for example, ask them to provide their street address and/or zip code.

ECHO USERS’ PASSWORDS WITH NONCHARACTERS

Use the HTML tag `<input type="password" />` for the password field. It instructs the web browser to echo users’ input as asterisks or bullets in the password field. However, because users don’t receive any feedback on what they are entering, when a login error occurs, remove users’ input from the password fields. In addition, ask them to check the “Caps Lock” key if passwords are case-sensitive.

WHEN NECESSARY, OFFER SECURE LOGIN

When allowing users to access personal information that is sensitive in nature, make the login process “secure” by transmitting the information over a Secure Sockets Layer (SSL) connection. Also, let users know they are logging in using a secure protocol (Figure 3.19). This can help increase users’ trust in the web application.

OFFER USERS AN OPTION TO REGISTER

Designers usually strive to make their web applications more convenient to repeat users and typically ask users to log in only when they need to identify

Sign in or create a Target.com account.

The image shows a web form for Target.com with two main sections: 'Returning Guests' and 'New Guests'. The 'Returning Guests' section includes a heading, a sub-header, two radio button options for signing in (Target.com account and Amazon.com account), and two text input fields for email address and password. Below these are two red buttons: 'Sign In' and 'Create a New Account'. There are also two links for forgotten password and email address changes. The 'New Guests' section includes a heading, a sub-header, and a red button for 'Create a New Account'. There is also a note about not needing a credit card to create an account.

Returning Guests

If you have an account with Target.com, please sign in.

I want to sign in with my:

☒ Target.com account.

☐ Amazon.com account. ([Learn more](#))

Your e-mail address:

Your password:

[» Forgot your password?](#)

[» Has your e-mail address changed since your last order?](#)

New Guests

If you don't have an account with Target.com, please create one.

[» Create a New Account](#)

You don't need a credit card to create an account. Payment information isn't required until you make a purchase.

FIGURE 3.20

Target offers users the option to register on the sign in (i.e., log in) page.

themselves. Considering that users may not have registered with the web application, it's important that they be offered an option to register (Figure 3.20).

ENABLE USERS TO RETRIEVE FORGOTTEN LOGIN INFORMATION

Users often forget their login information, especially when they do not access a web application frequently. Help users to retrieve forgotten login information by offering options such as “Forgot password?” and/or “Forgot username or password?” (Figure 3.21); see the FORGOT USERNAME/PASSWORD pattern later in this chapter.

CONSIDER A TWO-STEP LOGIN FOR HIGHER SECURITY

For security reasons, many financial applications require a two-step login to verify a user's identity. The first step is very similar to the login process described so far—that is, asking users to provide their username or user ID and password. The second step requires users to answer a security question. The answer must match the one provided during registration for them to successfully log in and access their account (Figure 3.22). Although many financial institutions require users to respond to a randomly selected security question, it may become annoying for users to answer security questions every time they log in. To minimize frustration, offer users the option to skip the additional step by registering the computer they typically use to log in.

Sign in to Yahoo!

Are you protected?
Create your sign-in seal.
(Why?)

Yahoo! ID:

(e.g. free2rhyme@yahoo.com)

Password:

☒ **Keep me signed in**
for 2 weeks unless I sign out. [Info](#)
[Uncheck if on a shared computer]

Sign In

[Forgot your ID or password? | Help](#)

Don't have a Yahoo! ID?
Signing up is easy. [Sign Up](#)

FIGURE 3.21 Yahoo! offers a “Forgot your ID or password?” link below the “Sign In” button and offers new users an option to register using a “Sign Up” link.

SINGLE SIGN-ON (SINGLE LOGIN)

Many web applications, especially business-to-business (that is, extranet) and business-to-employee (that is, intranet) applications, allow users to access one or more related applications based on their access rights. Such additional applications should be enabled for single sign-on (commonly referred to as SSO) so that once users have logged in, the same credentials are used to verify their identity with other applications. Users’ transition from one application to another should be seamless, and they should feel they are using the same application. For instance, once users have logged in to their Google Mail account, they do not have to log in again for accessing related applications such as Google Calendar and Google Documents.

CONSIDER ALLOWING THE USE OF “UNIVERSAL LOGIN” SERVICES

As mentioned earlier, allow users to log in using “universal login” services such as OpenID and Windows CardSpace (Figure 3.23). Such services allow users to create a unique digital identifier and use it to log in to any application supporting its use. This is similar to the SSO approach, except that users’ credentials are maintained by a third-party identity provider rather than the web application provider.

Cardmember Log In

Enter your User ID and password to access your account.

Primary Cardmember Information	
The information below is requested for your security and protection, and we keep it confidential. For more information, please	
User ID:	<input type="text"/> Required
Password:	<input type="password"/> Required
<input type="button" value="Log In"/>	
Forgot Your User ID or Password? Not Yet Registered? Need Help?	

(a)

Verify Your Identity

Please answer the security question below to complete your log in. Because we do not recognize this computer, we ask this question to ensure that your account information is kept safe and secure.

Answer Security Question:	
Security Question:	Answer:
In what city were you married? (Enter full name of city, e.g. Philadelphia)	<input type="text"/>
Remember this Computer: <input type="checkbox"/> Check this box if you would like us to remember this computer. You will not have to answer a security question if you log in with your User ID and Password on a computer we remember. You can have us remember as many computers as you like with your User ID and Password. <i>Note: You should NOT check this box if you are using a computer in a public area such as a library or Internet café or a computer you don't expect to use in the future.</i>	
<input type="button" value="Continue"/>	

SECURED BY
RSA

(b)

FIGURE 3.22 Advanta (a credit card company) asks users to verify their identity after they have logged in (a) by asking them to respond to one of the security questions they set up during registration (b). They also offer users an option to skip the additional verification step in the future by allowing them to let the application remember the computer they used to log in.

REMEMBER LOGIN INFORMATION

Like registering, logging in often distracts users from their goals and tasks. To minimize distractions, offer users the option to allow the application to remember their login information on their computers. Depending on the level of security and privacy concerns, such “remember me” options can be implemented in one of two ways:

1. *Remember both username and password* (Figure 3.24). This eliminates the login step completely for users as long as they use the same computer. Because browser cookies that are used to remember log in preference are stored on computers used to log in, users don’t have to log in as long as they access the application using the same computer or until the cookies expire or users delete them. For security reasons, the “remember me” function may be set to expire after a certain time period, such as two weeks or 30 days.
2. *Remember only the username* (Figure 3.25). This partial remembering option still requires users to enter their password to log in, but eliminates the need to enter their username. E-commerce applications

Login
Get in there and join the party.

Email
 Password

New to IconBuffer?
[Sign up for a free account.](#)
[Forgot your password?](#)
[Send an email to yourself with your password and login information.](#)

(a)

Login
Get in there and join the party.

OpenID lets you safely sign in to different websites with a single password. [Get an OpenID.](#)

OpenID URL

New to IconBuffer?
[Sign up for a free account.](#)
[Forgot your password?](#)
[Send an email to yourself with your password and login information.](#)

(b)

FIGURE 3.23 IconBuffer offers users the option to login with either a regular account (a) or with an OpenID (b).

Sign in to Gmail with your
Google Account

Username:

Password:

☒ Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#)
[New features!](#)

FIGURE 3.24
Gmail offers users the option to remember their login information.

(e.g., Amazon) typically use this approach and require users to enter their password before making any purchases.

When the security of user information is critical, as in financial applications (e.g., Fidelity, CitiCards), it's acceptable to trade-off user convenience for the prevention of misuse and identity theft and not offer the "remember me" option.

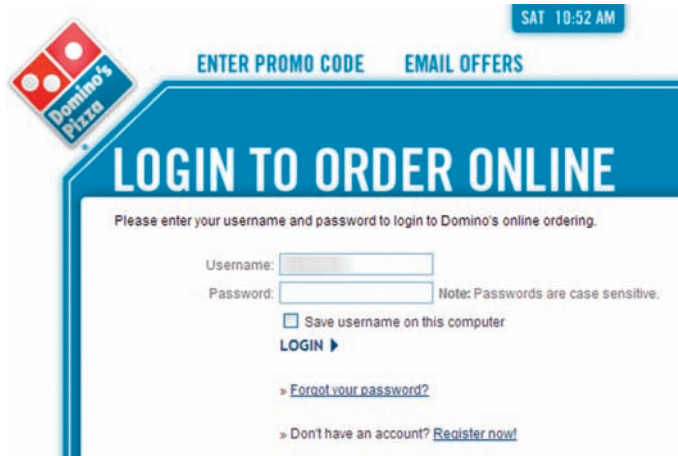


FIGURE 3.25 Domino's offers users the option to save their username on their computer.

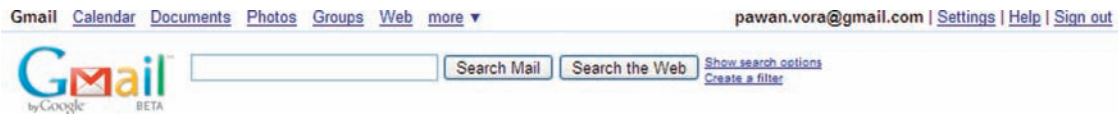


FIGURE 3.26 Gmail shows a user's email address along with a "Sign out" link in the top-right corner of the page to indicate that the user has successfully logged in.

CONFIRM LOGIN

Clearly indicate to users when they have successfully logged in. This may be accomplished by a "Welcome, username" message or by simply showing a username (typically placed at top right of the page; Figure 3.26). This is especially important when users have opted to be remembered on a computer.

LOCKING USERS' ACCOUNTS

When security is of utmost importance (e.g., finance applications), it is a reasonable precautionary measure to lock users out of their account after a certain number of unsuccessful login attempts. Users should be forewarned about this scenario after their first unsuccessful attempt (Figure 3.27). When locked out, users should be offered the phone number to call or the steps that they need to follow to unlock or reactivate their account.

Related design patterns

When asked to log in, users often realize they have forgotten their login information (FORGOT USERNAME/PASSWORD). In addition, if users have not created an account, they should be offered the option to set up one (REGISTRATION).

Log In or Sign Up

Existing Customers



We're sorry, your entry is not valid. Please check that the "Caps Lock" or "NumLock" key is off. Note: Fourth failed attempt will lock account access.

Please log in to view your accounts online:

User Name:
Password:
☒ Remember my User Name
LOG IN

- [Forgot your password?](#)
- [Need help with logging in?](#)
- [Protect yourself from fraud](#)
- [Questions about your account?](#)
- [Looking for Commercial Banking access?](#)

New Customers

Sign up now to:

Washington Mutual lets users know that their account will be "locked" after fourth unsuccessful attempt.

SIGN UP

- ▶ [Take an animated tour](#)
- ▶ [Is online banking safe and secure?](#)



FIGURE 3.27 Washington Mutual indicates to users that their account access will be blocked after the fourth failed attempt.

The LOG IN pattern is almost always accompanied by the LOG OUT pattern so that users can explicitly end their session with the application.

LOG OUT

Problem

After logging in and accomplishing desired tasks, users may want to end their session with the web application. They may want to do so for a variety of reasons:

- To prevent unauthorized users from accessing their personal information.
- To log out of one account and log in to another.
- To indicate that they have completed their task and no longer need access to the application.

Solution

Allow users to end their session by logging out (Figure 3.28).

Why

When users' account information can be misused, it's important that they be offered the option to log out. The ability to log out is particularly important for web applications because they are not installed on a specific computer and

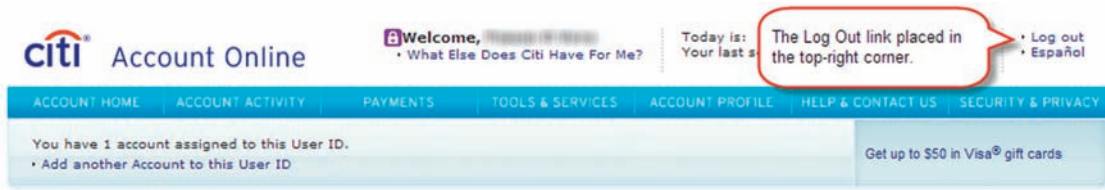


FIGURE 3.28 CitiCards offers a “Log Out” link to allow users to end their session.

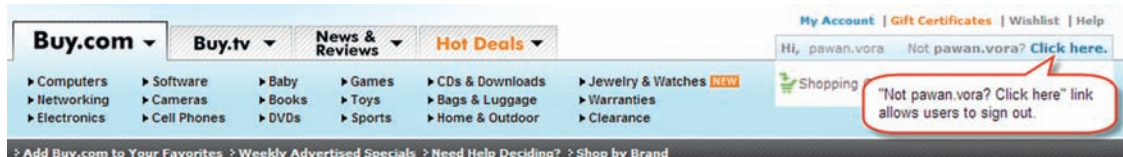


FIGURE 3.29 Buy.com uses a “Not pawan.vora? Click here” link to allow users to log out and log in as a different user.

are accessible from anywhere as long as users have access to the Internet and a web browser. On one hand, this offers users the flexibility to access their information from anywhere (e.g., libraries, shared computers at work, Internet cafes, and so forth), but on the other hand, this ease of access opens opportunities for misuse and fraud. Therefore, users must be offered an explicit way to end their session.

How

Offer users a log out option. Typically, the “log out” option is placed in the top-right portion of the page or closer to the username. Consumer web applications where login information is saved for future visits, especially e-commerce applications, do not offer an explicit logout but provide users with an option to log in as another user or offer options such as “Not username?” They greet users with the message “Welcome, username” to indicate that the user is recognized (Figure 3.29). When an explicit logout option is not offered to users, ensure that users have to log in for any financial transactions (e.g., checkout) or account updates (e.g., change password).

USE LABELS CONSISTENTLY

Although this has minor usability implications, a relevant design issue is labeling the action that ends user sessions with the application. The common options are logout, log out, sign out, logoff, log off, and sign off. As the link represents an action, appropriate usage is log out, sign out, log off, or sign off. In the absence of any research evidence, a common practice is to complement the action users used when accessing the web application: For most consumer applications, Sign Out (to complement Sign In) is used, and for many business and technical applications, Log Out (to complement Log In) is used.

ACKNOWLEDGE LOGOUT

Clearly indicate to users that they are logged out. The acknowledgment may be in the form of:

- A dedicated “You’re Logged Out” page with appropriate choices for users to navigate to.
- The login page with the appropriate message indicating that the user is logged out.
- A non-logged-in visitor version of the page (this is common on content portals such as Yahoo!, MSN, iGoogle, and so forth).
- A combination of these choices—for example, a dedicated page with an automatic redirect after a certain time delay (Figure 3.30).

The choice often depends on the “initial” conditions for login. If a user is required to log in to access the application, return users to the login page when they log out with a message acknowledging logout because that typically doesn’t require confirmation unless users are going to lose data. This also allows users to log in again if they logged out by mistake. Alternatively, if users started with a version of the page for non-logged-in visitors before logging in, then return them to a similar page when they log out.

Related design patterns

The LOG OUT pattern accompanies the LOG IN pattern because when users have to log in to access the application, they are usually offered the option to log out.

AUTOMATIC LOGOUT

Problem

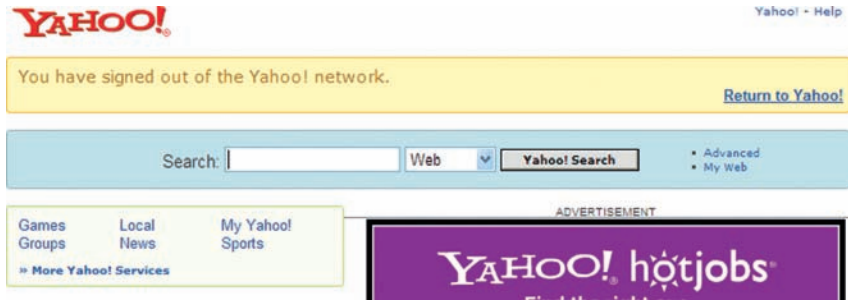
After logging in, users have stopped interacting with the application for a duration longer than expected, suggesting that they are either distracted or have abandoned the application but have forgotten to log out. By leaving their account in a logged-in state, users are exposed to misuse and abuse of their personal or sensitive data.

Solution

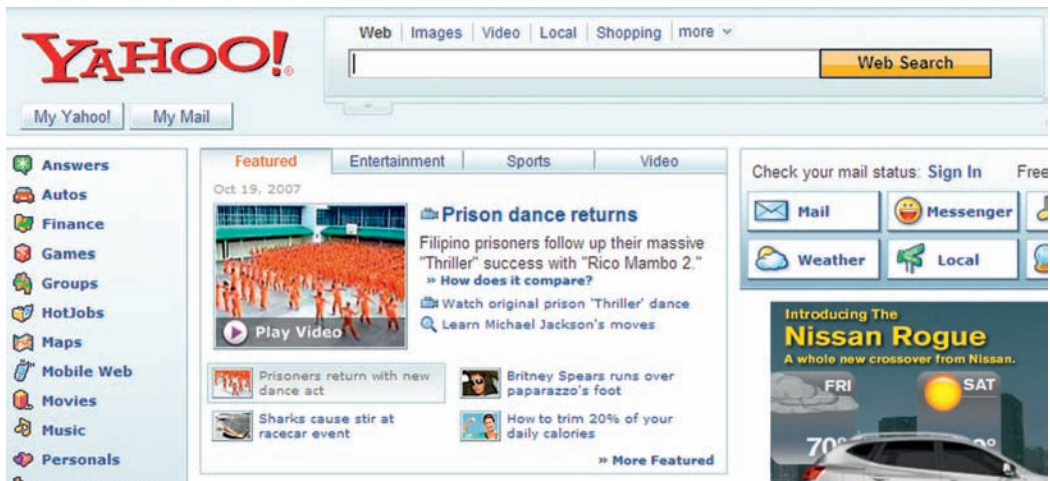
After a predetermined period of inactivity (e.g., 15–45 minutes), end users’ sessions by logging them out (Figure 3.31).

Why

Not only do automatic logouts help reduce the chances of unauthorized account accesses, but they also reduce the burden on the web server that maintains users’



(a)



(b)

FIGURE 3.30 Yahoo! uses a dedicated page indicating that users have signed out (a). After a brief delay, users are taken to the non-logged-in visitor version of the page (b).

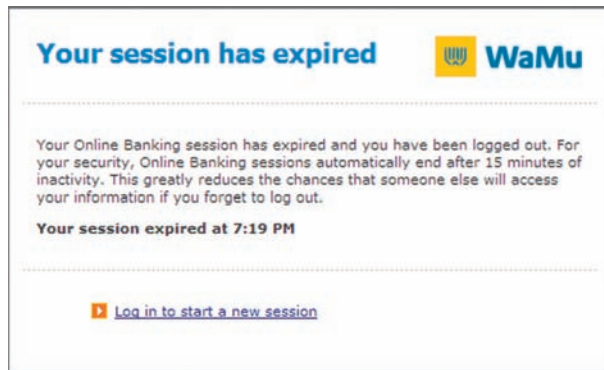


FIGURE 3.31 Washington Mutual logs users out after an inactivity period of 15 minutes. They also make it easier for users to start a new session by offering a link to log in again.

session information. Automatic logouts are particularly important with new browsers, which allow tab-based browsing. Many users open multiple tabs and access several web applications and often forget to log out of their sessions.

How

For applications with security and/or privacy concerns, automatically log out users after a certain period of inactivity (i.e., session timeout). Typical session timeouts are 15- to 45-minute durations depending on the sensitivity of the data that may be exposed. As the session timeout is approaching, offer users a warning and give them an opportunity to stay logged in. Confirmation is especially useful in instances where user tasks are likely to take some time (e.g., in cases of multistep tasks like checkout) and likely data loss could be frustrating to users (Figure 3.32).

When session timeout occurs, the following are quite common:

- Users are taken to the Login page with a message that the session timed out (or suspended) and that they must log in to start a new session. This approach is useful when the data available on the screen are sensitive.
- Users are kept on the same page with a pop-up that indicates that the session was suspended and whether or not their data were saved (say, for example, in a “draft” status). This approach is not recommended when data available on the screen (behind the pop-up) are personal and/or sensitive.

For some applications, sessions can end if the browser window used to access the application is closed.

SAVE USERS' INFORMATION

When automatically logging out users, consider saving their information. It could be annoying for users to have their session time out and discard all their data when they intended to finish what they started but were distracted for



FIGURE 3.32 As session timeout approaches, Bellco prompts users and offers them an option to continue their current session. It also shows how users can change the session's timeout duration.

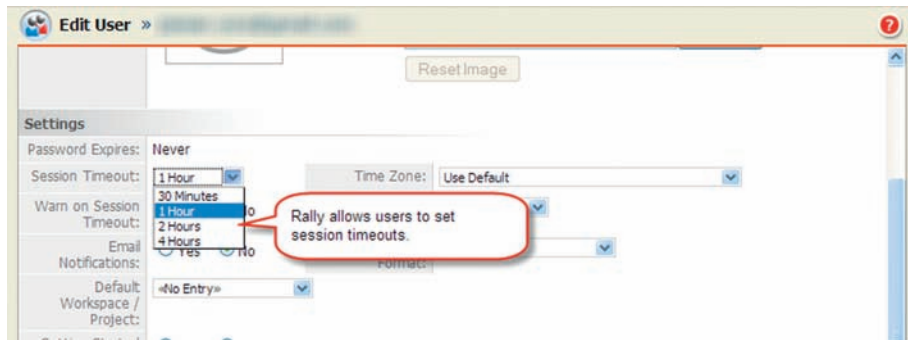


FIGURE 3.33 Rally Community Edition allows users to set their session timeout duration for up to four hours. The default timeout is set to one hour.

some reason. For example, Gmail saves users' incomplete emails in the "draft" state and marks them to indicate that they have a pending response.

ALLOW USERS TO SET DURATION OF SESSION TIMEOUTS

Users may want some web applications to have longer or shorter session timeout duration than the one defaulted by the application. This is common for applications that users may use all day, such as email, office productivity applications (e.g., word processing, spreadsheets), and status-monitoring applications (e.g., investment tracking). If timeouts are set for such applications, offer users an option to change the duration (Figure 3.33).

Related design patterns

AUTOMATIC LOGOUT is a fallback measure where users may forget to log out and therefore expose personal or sensitive information. It's quite possible that users may not know how to log out of an application because the available option is hidden or not located where users expect it to be (LOG OUT).

FORGOT USERNAME/PASSWORD

Problem

Users often forget login information (username and/or password) and without it are unable to access the application.

Solution

Offer users options to remember or retrieve forgotten login information (Figure 3.34).

Why

Users often forget usernames and/or passwords, especially when they are accessing an application that they rarely use. Therefore, it's important that users

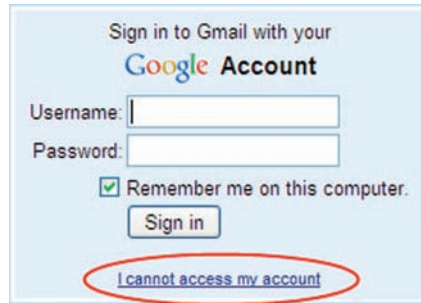


FIGURE 3.34 Gmail offers an “I cannot access my account” link.

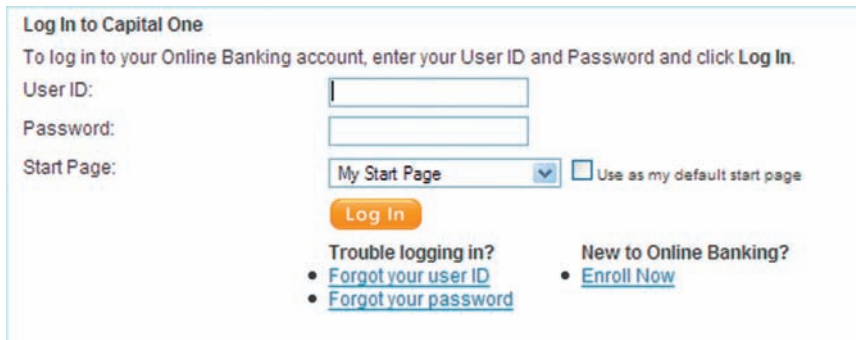


FIGURE 3.35 Capital One offers links for “Forgot your user ID” and “Forgot your password” below the Log In button.

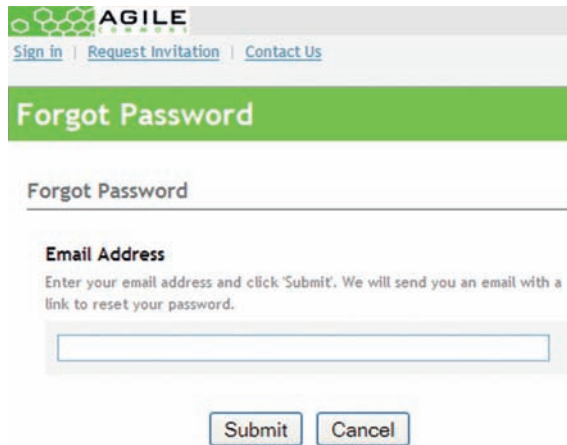
have a way to remember that information or retrieve it. Because users typically realize that they have forgotten their credentials when asked to log in, the options to retrieve them should be provided near the login area. In situations where user accounts are not tied to private or sensitive information, sending a link to reset passwords via email is acceptable. However, when dealing with sensitive information, it’s important to take additional steps to verify identity before allowing users to reset or access their log in credentials.

How

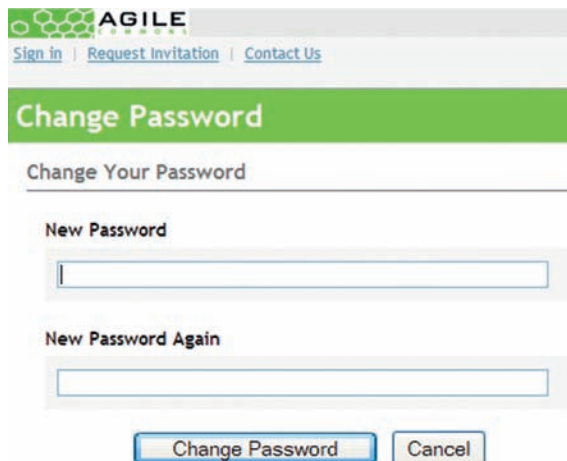
Provide a “Forgot User ID (or Password)” link near the login area (Figure 3.35); if users’ email addresses are used for logging in, the “Forgot Password” link is sufficient.

SEND PASSWORDS TO REGISTERED EMAIL ADDRESS

If the web application being accessed doesn’t store personal information about users that can be misused (e.g., health-related or financial information), ask users to provide their username or the email address they used to register. Once verified, passwords can be emailed to them. For improved security,



(a)



(b)

FIGURE 3.36 Agile Commons (hosted by HiveLive) emails the link to reset the password after verifying the email address (a). Clicking the link displays the reset password page (b).

instead of emailing the current password, assign users a temporary password that they can change as soon as they log in. Alternatively, users may be emailed a link to reset their password (Figure 3.36).

CONFIRM USER IDENTITY WITH SECURITY QUESTIONS

If the web application stores sensitive information, additional layers of security may be necessary to verify the identity of the user claiming to have lost log in information. Additional identification questions may include information that only the account owner knows, such as the last four digits of his or her Social Security number, account number, and so forth (Figure 3.37). The identification

Forget Your User ID or Password?

Please submit the form below to retrieve your User ID and select a new password.
If you are a Delegate for this account, [click here to retrieve your User ID](#).

Step 1: Primary Cardmember Information

The information below is requested for your security and protection, and we keep it confidential. For more information, please read our [Privacy Policy](#).

Your Advanta Card Number:

(Enter the account number that appears on your Advanta Business Card, not on your monthly billing statement.)

Your 4 Digit Expiration Date (Ex. 01/05): /

Enter the Last 3 Digits of Your Signature Panel:

(See example above)

Last 4 digits of Your Social Security Number:

Enter Your Date of Birth (Ex. 11/18/2005): / /

FIGURE 3.37 Advanta, a credit card company, asks for several identification-related questions before resetting user ID and password.

may also require users to answer one or more security questions set up during registration.

Related design patterns

Users may realize that they have forgotten their username and/or password when they are prompted to log in. Therefore, options to retrieve them should be presented along with fields that are required to log in (LOG IN).