Online Credit Card Processing

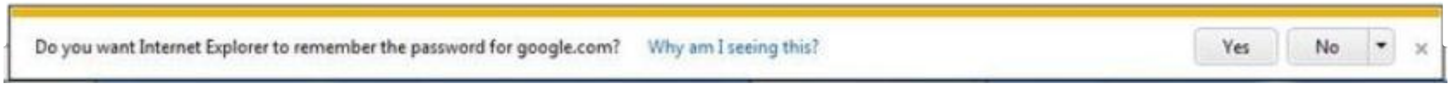
PRECAUTIONS FOR CREDIT CARD SECURITY

InfoPathways, Inc.
www.infopathways.com
25 Liberty Street
Westminster, MD 21157
(410) 751-9929 TEL
(443) 244-9951 FAX

The weakest link in the credit card paying process is the company that processes payments.

CAUTION WHEN SAVING INTERNET HISTORY

Do not save credit card information online. Some web pages may ask you to save your credit card information for future purchases. Do not do this as someone can go back to that web page and have a shopping spree at your expense.

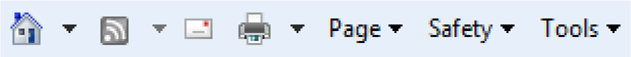

Do you want Internet Explorer to remember the password for google.com? Why am I seeing this?

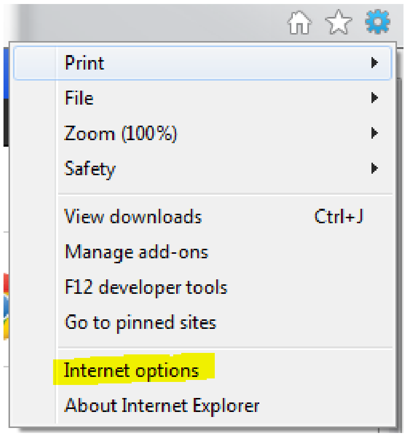
Most online accounts remember your Username and give you the option to save your Password. If you have a password saved, the account's history will automatically fill in the password after selecting the Username option. This is the same for entering credit card numbers! If a web user logs into a shopping site you previously visited on the same computer and decides to purchase something, they might be able to use the same trick and select a credit card number that drops down. Any time you use a public computer, never set the account to save your Passwords and ALWAYS log out upon completion of your tasks. If you simply exit out of the web browser, the next user can reopen the web page and be automatically logged in as you. There is usually a set timeout period in which a user can stay logged in if not active. This timeout period creates a window in which a malicious user can navigate to that site and use it as if they were you. Have you seen Facebook pages "hacked" by the user's friend in which they post embarrassing status updates? It's the same idea, but with your credit card and your private information.

CLEARING SENSITIVE INFORMATION

If you are worried about saved usernames and passwords, there is a way to erase that memory from your computer. Before doing so, note that it will erase MORE than your usernames and passwords. When you are ready, follow these steps below:

1. In your browser (Internet Explorer is used in this example), you may have a small tool bar; click the tools button in the upper right-hand corner (shown below) and select "Internet Options". In other set ups, you may just see a small gear icon (shown right) to access the same option.

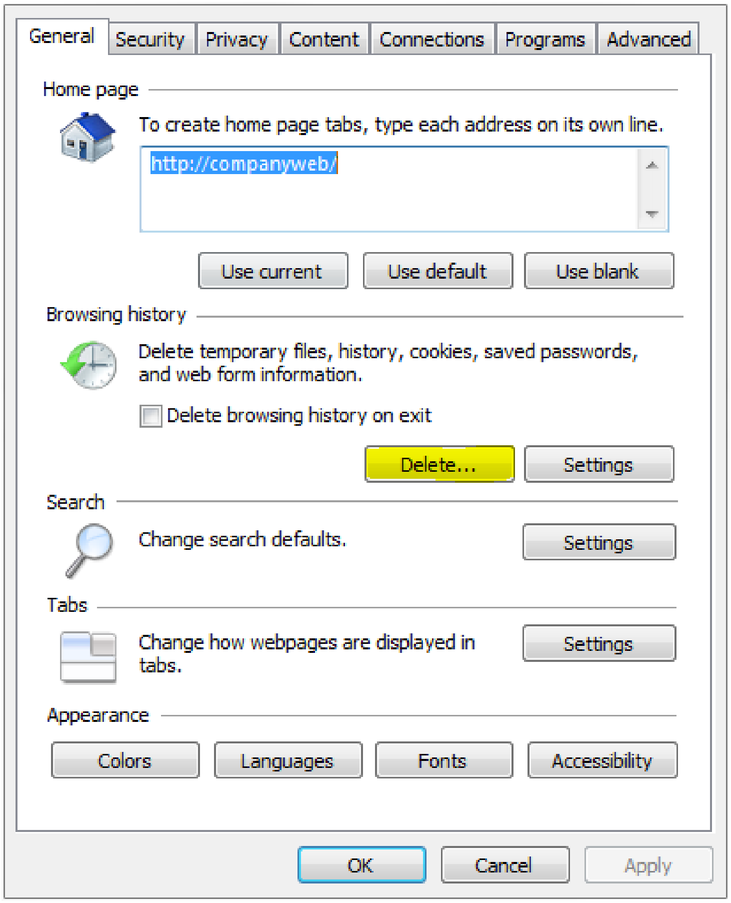




2. Under the "General" tab of the "Internet Options" window (next page, left), select Delete to bring up the "Delete Browsing History" window.

3. In the "Delete Browsing History" window (next page, right), select what data you want to delete.

   Before doing so, note that certain selections will erase MORE than your usernames and passwords. It can delete temporary files, history, cookies, saved passwords and web form information. After a thorough clean-up, you may find that some processes that were automatic now have to be completed manually (like typing out full website addresses and populating online form fields that you may fill out on a regular basis).



Home page

To create home page tabs, type each address on its own line.

http://companyweb/

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

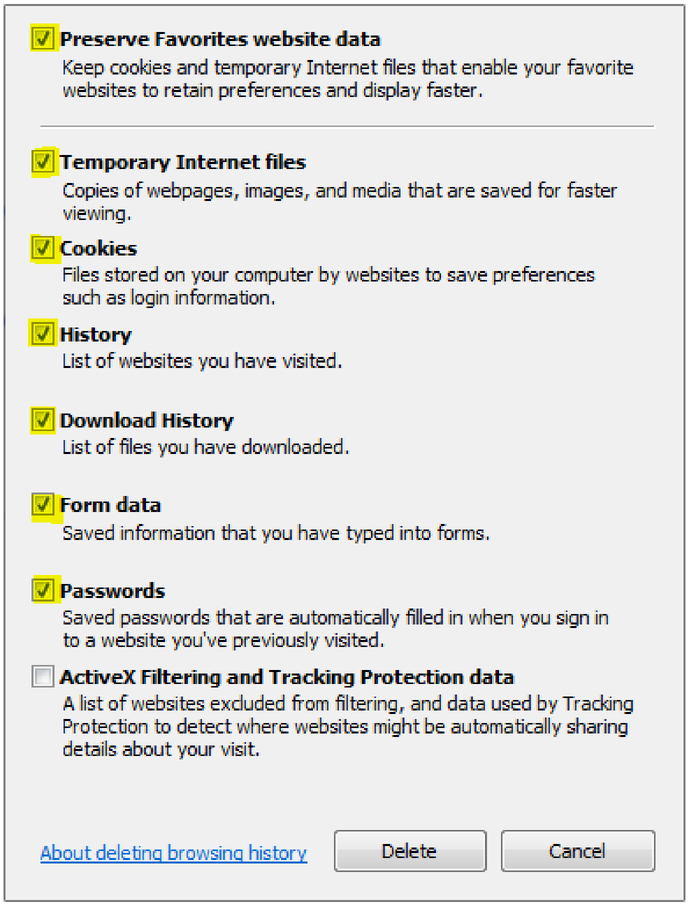
Search

Change search defaults.

Tabs

Change how webpages are displayed in tabs.

Appearance



☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

☑ **History**
List of websites you have visited.

☑ **Download History**
List of files you have downloaded.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

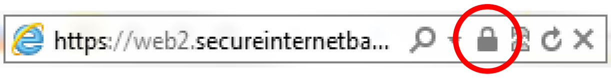
□ **ActiveX Filtering and Tracking Protection data**
A list of websites excluded from filtering, and data used by Tracking Protection to detect where websites might be automatically sharing details about your visit.

SAFE PRACTICIES

Never send credit card or password information unencrypted via email, txt, instant message, picture or video. Information can be intercepted using online communications. If you are worried about one of your accounts, change your Password. All accounts provide this service, and it is certainly not a bad practice to periodically change your passwords.

Finally, monitor your credit card statements regularly. Checking your statements is not limited to mail or logging into the bank web page. Banks and credit card companies have developed (or have begun developing) smartphone applications allowing you to check your statements quickly, easily and very securely.

If you are making a purchase online, a good way to tell that the site is secure is if the website address begins with "https rather than "http". Https allows for secure ecommerce transactions, such as online banking, by encrypting the session with a digital certificate. Internet Explorer and Firefox display a padlock icon to indicate that the website is secure.



As Julianne Pepitone for CNN news writes, ***"For customers, the best thing to do is sit tight. If your card issuer thinks your account may have been compromised, they'll contact you -- and no matter what, you're not liable for unauthorized charges made on your account."***

And Visa reassures ***"It's important for U.S. Visa consumer cardholders to know they are protected against fraudulent purchases with Visa's zero liability fraud protection policy, which exceeds federal safeguards. As always, Visa***

encourages cardholders to regularly monitor their accounts and to notify their issuing financial institution promptly of any unusual activity."

The consumer is somewhat protected but, the more you ignore internet security, the less financial institutions can do to help you. Protect your accounts, your credit card information, and follow safe practices for online purchasing.