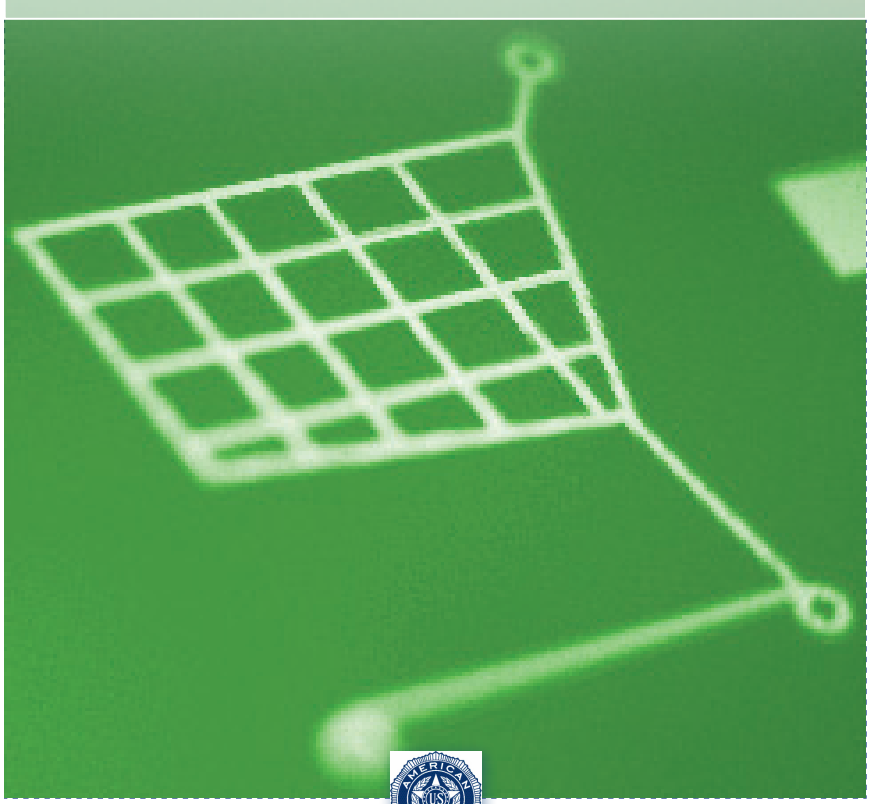
THE AMERICAN LEGION

A LEGIONNAIRE'S GUIDE TO THE WEB

ISSUE 3: ONLINE TRANSACTIONS

Cybershopping – safe and secure



Shopping online: *Convenient, smart and safe.*

Convenient – Find products that a
available locally, comparison-shop
search engines, and have your
orders delivered to your door.
Discounted online prices often
make up for shipping fees, and
some merchants even offer free
delivery. *(With some merchants,
airlines, you might even pay extr
don't buy online.)*

Smart – Research before you
Merchant sites often post
extensive information about
their wares, from specs to
size charts to country of
origin. Customer reviews
provide food for thought
about the products and hc
the company treats its cus

Safe – Security features e
your "Web browser" – the
(Internet Explorer, Safari, Fi
gets you on the Internet – make
give a website your credit-card info than to
hand the card over to a real person. The FBI and
the Federal Trade Commission (FTC) both say
that the vast majority of identity thieves still work
the old-fashioned way – copying numbers when
processing your card, bribing employees, stealing
wallets and going through trash.

Online shopping does have its downsides: you
can't touch the stuff you're buying, and it takes
longer to get it; it takes longer to return, and
dealing with customer service via email can be
frustrating.

Commerce reports that
online retail sales totaled
$165 billion in 2010 –
a 15-percent increase
from the year before.
Significantly, e-commerce
sales outperformed
total retail sales, which
increased only 7 percent
in 2010.

If you think your information has been stolen

First, limit your exposure

■ Contact your credit-card company promptly.

■ Call or email the customer-service department of the website where you made the transaction *(or, if you suspect "phishing," where you thought you made it).*

Then, blow the whistle by filing a complaint

Internet Crime Complaint Center
http://www.ic3.gov/complaint/default.aspx

Federal Trade Commission (FTC)
https://www.ftccomplaintassistant.gov

(877) ID THEFT (877-438-4338)

Consumer Response Center, FTC
600 Pennsylvania Ave. NW,
Washington, D.C. 20580

Purchasing Safely Online

■ **Protect your information.** You should never provide your number, or any personal information, to someone who solicits you via email. This is known as "phishing." Phishing scams can be pretty sophisticated, including fake websites that look legitimate. Protect yourself by not participating in any transaction yc didn't initiate yourself. If you get a email asking you to update your account information, report it to the company before providing anything.

■ **Know your merchant.** Legitimate online vendors pay to be vetted by "certification authorities" that guarantee the vendors are who they say they are. The logo of the certification authority is usually displayed somewhere on the website; common ones are *VeriSign* and *eTrust*, but there are dozens of others, and many sites have multiple certificates. Clicking the logo opens a window with more information about the certificate. As an example, take a look at the ***Legion.org*** membership-renewal page – it prominently displays the *VeriSign* icon.

■ **Keep your receipt.** Get a receipt, and hang onto it until you get what you bought and you're sure it's satisfactory. According to the Internet Crime Complaint Center, simple nondelivery of goods is by far the most common online-shopping fraud complaint.

■ **Speak up.** Don't hesitate to call or email the merchant, or contact your credit-card company, if you have any doubt about a transaction.

Your Browser Protects You

The Internet was built for speed. When you click "Submit Order," the form you filled out is broken into "packets" that race all over the Web to the merchant's computer, where they are reassembled. All that would-be snoops see is gibberish, because the contents are encrypted – and for this you can thank your Web browser.

When you land on a site's order page, your browser "requests" a secure session. The browser and the merchant's transaction computer then agree on an encryption key*, or secret cipher, to code all the communications for this transaction only. It's discarded once the transaction is finished or after just a short time, as anyone who has been called away while buying something has found when they had to start over.

Generating the cipher, called public-private key encryption, involves gigantic prime numbers. But it happens so fast, you'll never know it's going on. There are a few clues, however:

■ **Look for "HTTPS."** If the Web address, or URL, of the page starts with this, that indicates the page is being encrypted. *(Regular-page URLs start with "HTTP.")*

■ **Look for the lock.** Many browsers display a lock icon in the status bar of a secure page. *(Make sure your browser's status bar is turned on by checking it under "View.")* Sometimes you can click the icon to get the page's security status. Clicking also displays the site's security certificate, which is an indication that your browser is staying up-to-date on all certification authorities. (If you start a transaction with an online merchant that does not have a security certificate, your browser will warn you.) You need to make sure your browser is updated regularly with this information, so if your computer asks if it's OK to update, say yes!

*Encryption education

For more information on how public-private keys work, search the Web for **"asymmetric encryption."** The government uses it, and it's also how your email stays private.

Double check the locks

On most websites, only the most sensitive pages, such as login screens, registration pages and order forms, have HTTPS addresses. So don't worry if you don't see the HTTPS or the lock on every page; just make sure it's there when you start tapping in your credit-card number.

About Cookies

Internet crime by the numbers

The Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center. According to IC3:

2 million | Complaints received since 2000

303,809 | Complaints received in 2010

121,710 | Complaints referred to law enforcement in 2010

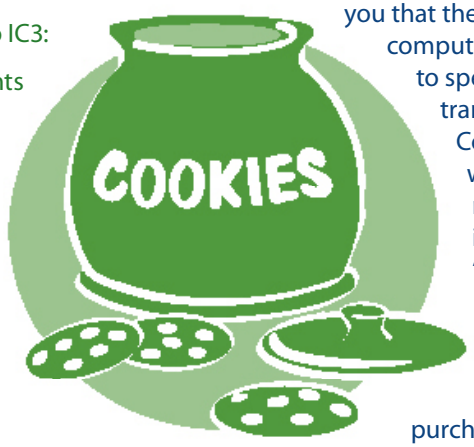
14.4 | Percentage of 2010 complaints about nondelivery of payment or merchandise

13.2 | Percentage of 2010 complaints about scams using the FBI's name

9.8 | Percentage of 2010 complaints about incidents of identity theft

Wikipedia quotes a 2007 U.S. Government Accountability Office (GAO) study of data breaches saying that "most breaches have not resulted in detected incidents of identity theft."

You may have heard of cookies. In computer parlance, a cookie is a string of computer code attached to your browser, and thus to your computer's hard drive, by a website. This is usually not a bad thing. Cookies identify you to sites you've already visited, and may store (or reference) information about you that the merchant's computer can use to speed your transaction. Cookies are also why when you revisit a site, it might say, "Hello, want to buy some ink to go with that printer you just purchased?"



Cookies may let a merchant keep track of what you're doing on the site – which pages you hang around on, and which you dump out of immediately. This helps the people who run the site improve the visitor experience. (If you read the ***Legion.org*** Privacy Policy, you'll see that this is exactly what's happening.)

Cookies CANNOT read or convey anything from your hard drive, and they cannot act as a conduit for other programs to get access to your information. You can delete them from your computer any time you want. You don't have to accept them, but some websites won't do business with you unless you have a cookie at least during your current transaction.

Privacy and Legion.org

Reputable websites post their privacy policies. The policy for Legion.org is at ***www.legion.org/privacy*** – you can link to it by clicking "Privacy Policy" at the bottom of any page.

You'll see that ***Legion.org*** collects both "Active Information" – the data you enter yourself, such as when you register – and "Passive Information," which is collected automatically while you use the site.

Other registered users can see the "Active Information" in your ***Legion.org*** profile unless you opt out in the site's Privacy Settings. This information may also be used to send you emails about products, promotions and other information. Again, you can opt out if you don't wish to receive these emails.

The VA Benefits Calculator does not store any of the information you provide; it is discarded after each calculation.

Passive Information, such as what pages you visit and how long you stay, is collected automatically whenever you are on the site. This data is never connected to your personal information or email address, but is compiled or "aggregated" so that it can be used to administer the website and provide information to advertisers about user habits and characteristics.

Legion.org does not rent or sell users' personal information, although it may have to be disclosed in certain instances, such as when necessary to comply with law enforcement.

Safe surfing

Secure online transactions make it easy to take advantage of American Legion programs and offers. Here's a sample of what you can do:

- **Join the Legion**
- **Renew your membership**
- **Make a donation**
- **Purchase items from the Legion's Flag & Emblem catalog**
- **Register and update your post's baseball team**
- **Buy subscriptions, publications and reference materials**
- **Patronize advertisers**
- **Join USAA**

THE AMERICAN LEGION

P.O. Box 1055 • Indianapolis, IN 46206-1055

STOCK # 45-003