FBI Omaha Counterintelligence Strategic Partnership Program

November/December 2011
Volume 2, Issue 4

Federal Bureau of Investigation

4411 S. 121st Court

Omaha, Nebraska 68137

Executive Management

- **Weysan Dun**, *Special Agent in Charge*
- **James C. Langenberg**, *Asst. Special Agent in Charge, National Security Program*
- **Edward C. Reinhold**, *Asst. Special Agent in Charge, Criminal Program*

Inside this issue:

Most popular shopping sites

Amazon.com	eBay	Shopzilla
PriceGrabber	Overstock.com	Nextag
Buy.com	Craigslist	Half

Sources include ecommerceoptimization.com, blogspot.com and listofsearchengines.info

Questions about the Omaha Field Office Counterintelligence Strategic Partnership Program:
Special Agent Mary T. Dolan, Strategic Partnership Coordinator
402.530.1251 (desk); 402.250.3389 (cell); Email: Mary.Dolan2@ic.fbi.gov

Best ways to stay safe online

1 **Activate protection.** If your operating system or software has a firewall, spam blocker, or other built-in security application, make sure it's turned on. The firewall included with Windows Vista is adequate. The Mac one is lacking, but Apples are generally less targeted by hackers. ZoneAlarm 7.0 is a free firewall for Windows XP. Search for the operating system security application at *www.download.com*. Also activate spam filtering and other online protection provided by your ISP or e-mail service, such as Yahoo, Google, or MSN. For spam, that may be enough.

2 **Update and renew.** Set your operating system and security software to update automatically. Spam, spyware, and virus-detection programs incorporate "rules" or "definition" files that must be updated regularly to catch the latest threats. If your computer remains disconnected from the Internet for long periods, you should ensure that automatic updates to your operating system security are occurring, or update manually. And when your software warns you to renew your service, be sure to do so, ensuring that protection doesn't lapse.

3 **Upgrade your computer and browser.** If you're running Windows XP or earlier Windows versions, consider upgrading to the more secure Windows Vista, which lets you surf in a protected environment that prevents online threats from damaging your operating system and contains a two-way firewall that blocks both incoming and outgoing threats. (The outgoing firewall needs some improvement to make it more effective.) At a minimum, upgrade to the Internet Explorer 7 or Firefox 2 browser. Both notify you about known forged, or "phished," Web sites.

4 **Install a toolbar with security features.** We haven't formally tested these supplementary online tools, but we think they're a good second line of defense. The EarthLink Toolbar (*www.earthlink.net/software/free/toolbar*), for example, incorporates a scam and popup blocker, spyware scan, and home page protection. The Netcraft antiphishing toolbar (*www.toolbar.netcraft.com*) warns about known phished sites and can reveal a site's hosting company and even its registered owner. If you go to sites after installing McAfee Site Advisor (*www.siteadvisor.com*), the program lets you know whether McAfee tested it and, if so, what it found, including viruses, spyware, spam, pop-ups, phishing, and consumer scams. It even overlays its site reports on Web search results and automatically blocks access to sites that exploit browser weaknesses.

5 **Shut off your computer.** Turning off your computer when not using it for long periods (or at least disconnecting the Internet cable) can reduce the chance that a malicious remote computer will penetrate your operating system security and access it. And you'll save energy.

6 **Use public computers with care.** Avoid using computers at libraries, hotels, or airports for conducting financial or other personal business. The same goes for using your own computer on a public wireless network, especially if you're not on a secured Web page or haven't disabled your system's computer-to-computer connections.

7 **Consider a Mac.** Although Mac owners face the same problems with spam and phishing as Windows users, they have far less to fear from viruses and spyware. Because Apples are less prevalent than Windows-based machines, online criminals get less of a return on their investment when targeting Macs.

8 **Watch what you download.** The myriad of free utilities, games, and other software on the Internet can be useful, but many are laden with viruses and spyware. Try to download only from well-known manufacturers or trusted sites such as those at *www.download.com*, *www.snapfiles.com*, and *www.tucows.com*.

9 **Consider a suite.** For a simple route to broad operating system security, select one of the security suites recommended on page 36. Just remember that you might be paying a premium to duplicate some components already on your machine or available free. We recommend having at least a gigabyte of memory to prevent the suite from slowing down your computer.

10 **Run antivirus software.** It actually works and you need it. That's true even if you own a Mac. Although Mac users have much less to fear from viruses and spyware, they aren't immune to them. And an antivirus program will prevent virus-laden files from being transferred from Macs to PCs.

11 **Run two antispyware programs.** Spyware is so insidious, and sometimes difficult to detect, that it warrants double protection. Set the better of the two programs to block spyware in real time. Use the other to scan whenever you suspect something might have escaped the first program.

12 **Use 'disposable' e-mail addresses to thwart spammers.** If spam's a problem, consider using disposable addresses for different purposes. For example, use "smithshopping08" for buying online. If that address starts getting spam, abandon or change it. Many ISPs provide extra "associate" e-mail addresses that you can change at will. For convenience, configure your e-mail program to check all your addresses simultaneously. Or set up disposable accounts at a free e-mail service such as Google or Yahoo. A caution: Guard the primary e-mail address you got from your ISP, because you can't change that one without abandoning your entire account.

13 **Use a credit card.** Credit cards offer better protection than other options when shopping online. Even better, some issuers let you generate virtual account numbers that are valid for a single purchase with a fixed dollar limit. Use those and you won't have to give online retailers your permanent card number.

14 **Don't assume a certified site is safe.** Although it's vital to have a secure connection when sending personal information online (indicated by "https" before the Web address and a padlock or other icon on your browser), it's no guarantee the Web site is reputable. Similarly, certification symbols from the Better Business Bureau, TRUSTe, and similar organizations provide some reassurance (assuming they're being used with authorization). But they're no substitute for reading the fine print and researching a site by talking to friends and checking online reviews before turning over credit-card or other information.

15 **Guard personal information.** Never respond to e-mail requesting your passwords, user names, Social Security number, or other personal information, no matter how official it looks. If you're asked to call a telephone number, verify it independently.

16 **Avoid using hyperlinks in e-mail.** Hyperlinks can show one address but take you to another. Before clicking on links in Web pages, hover your cursor over the URL and see whether the address that appears at the bottom of your browser looks as if it's related to a page or site you expect to visit. When you arrive at the site, verify that the URL shown in your browser's address bar is the correct one. Pay attention to the part of the URL between "http://" (or https://) and the next slash. Look for tricks such as the use of a zero where the letter O should be. Verify the address and then type it into your browser. Or use a favorite or bookmark you've already stored in your browser.

17 **Type carefully.** Tricksters sometimes create lookalike sites that use common mistypings of popular URLs.

18 **Report phishing.** If you receive a phishing e-mail, forward it to the Anti-Phishing Working Group (*reportphishing@antiphishing.org*), the Federal Trade Commission (*spam@uce.gov*), and the company or organization that is being impersonated. You also can file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov. If your anti-phishing toolbar doesn't recognize a fraudulent Web site, report the site to the toolbar provider.

19 **Review your accounts regularly.** Review your credit-card and bank statements as soon as you receive them. Report suspicious charges or withdrawals immediately.

10 Tips for Shopping Safely Online

Things to Check on Before You Click Checkout

By Andy O'Donnell, About.com Guide

Whether you're shopping the holiday sales, or just looking to avoid the craziness at the mall, shopping safely online can be a challenge, especially if you stray from the larger e-tailers to get a better deal from a lesser known site. Here are 10 tips to help you gain some peace of mind while shopping online.

1. Check the seller's customer satisfaction ratings

Other people's experiences with the merchant that you are considering are often an excellent gauge of what to expect when you order. Review other user's comments and check out the seller's rating on sites like Google Shopping. Low "star" ratings may provide a red flag that cautions you to find a more reputable seller.

2. Check the Better Business Bureau site to see if there are a large number of complaints about the seller

The Better Business Bureaus of the United States and Canada are excellent resources to find out specific information about merchants, including whether or not they have any complaints against them related to delivery, product issues, or refund or exchange problems. You can also obtain their business addresses and corporate contact information, which might allow you to circumvent the frontline call center circus of endless automated prompts (i.e. "Press 1 to speak to a semi-live person").

3. Whenever possible, use a credit card for payment

According to the American Bar Association's website, safeshopping.org, it is best to use a credit card when paying online because federal law protects credit card users from fraud and limits individual liability to $50. Some card issuers might even waive the $50 liability fee or pay it for you.

Consider opening a separate account for buying online so your online purchases don't get lost in the sea of Starbuck's coffee transactions in your online banking ledger. Also, look into virtual credit cards if your card issuer offers this service. Some card issuers will give you a one-time use virtual card number that you can use for a single transaction if you are concerned about the security of a particular merchant.

4. Never enter your credit card information on a page that is not encrypted.

When using the online checkout process of a seller, always make sure that the web address has "https" instead of "http." Https ensures that you are using an encrypted communications path to transmit your credit card information to the seller. This helps to ensure against eavesdropping on your transaction.

5. Go directly to the seller's site rather than clicking a "coupon" link that was sent to you by an unknown source.

Scammers can often use a tactic called cross-site scripting to craft a hyperlink that appears to be the actual merchant site but actually relays your credit card information to the scammer when you put your payment information into the payment web form. Unless you can verify that a coupon came from the actual vendor's site to which you have already subscribed, it's best to avoid random coupons with unknown origins.

6. If you are ordering from a shared computer (i.e. the library, computer lab, or a work PC), log out of the shopping site and clear the browser history, cookies, and page cache.

This seems like a no-brainer, but if you're using a shared machine, always log out of the store website and clear your browser's page cache, cookies, and history when you are finished ordering something, or the next guy who sits down at the PC you were using might just have himself a little shopping spree on your dime.

7. Never give your social security number or birthday to any online retailer.

Vendors should never ask you for your social security number unless you are applying for in-store financing or something to that effect. If they are trying to require you to enter a social security number just to order a product, then they are most likely scammers. Run away fast. While your birthday may seem like an innocent enough piece of data to give out, it's just one more of the three to four data elements needed by a scammer to steal your identity.

8. Find out the seller's physical address.

If your seller is in a foreign country, returns and exchanges may be difficult or impossible. If the merchant only has a P.O. box listed, then that may be a red flag. If his address is 1234 in a van down by the river, you may consider shopping elsewhere.

9. Check out the seller's return, refund, exchange, and shipping policies.

Read the fine print and watch out for hidden restocking fees, crazy high shipping charges, and other added fees. Beware of "coupon clubs" that the seller might try to get you to sign up for during your purchase. These clubs may save you a few dollars, but often they involve monthly billing for the privilege of joining.

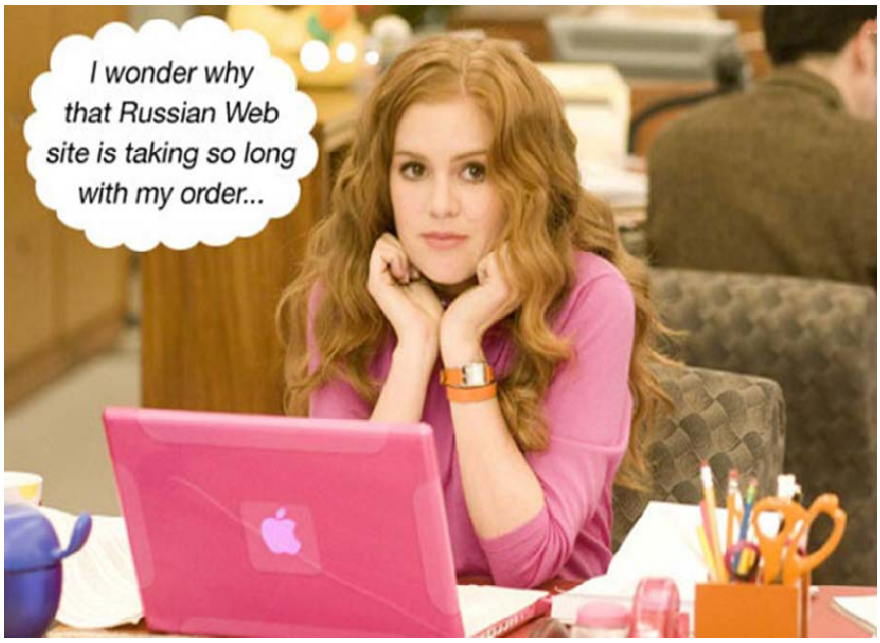
10. Check the seller's privacy policy.

While we might not think about it, some sellers resell our personal information, buying preferences, and other data to market research companies, telemarketers, and spammers. Read carefully and always make sure that you are opting-out and not opting-in when asked whether you want to have your information shared with "3rd parties" (unless you like a lot of spam in your e-mail). You may also want to obtain a separate e-mail account to use while shopping online to avoid clogging up your personal e-mail box with the barrage of sale ads and other junk mail that is frequently sent out.

Be smart, be safe, and know that there are groups such as the Internet Crime Complaint Center that can help you if you think you've been outright scammed. Check out our other resources below on how to shop smart.

Fake Sites

Phishing isn't just a bank problem anymore. Scammers aiming to steal your personal account and financial information are increasingly masquerading as web companies like Amazon.com, EarthLink and eBay. Their cover: legit retailer sale spam, which increases 20% as the holiday season approaches, reports web security firm MX Logic. "During those times of the year when you're doing extra shopping, you have to be especially vigilant," says Beth Givens, director of the Privacy Rights Clearinghouse. "If the timing is just right, you've just made a purchase; the phishers' message could get you at a vulnerable moment."
Worse, you don't even need to enter your information on the scammers' fake site to become a victim. More phishers are embedding data-stealing spyware that downloads to your computer as soon as you click on one of the embedded links in the email.



Protect Yourself: Ignore the dire warnings of an account shutdown. "You have to realize that companies are not going to do business that way," says Givens. Don't even follow the link. Open a new Internet browser window and type in the company's real web address. From there, you can log into your account to check for alerts, or look for the toll-free customer service number to address the problem if there even is one.

FTC offers guidelines to reduce online shopping risks

By Jeremy Kirk
November 21, 2006 12:00 PM ET

IDG News Service - Online merchants may be ready for holiday season Web orders this year, but Grinches will also be on the Internet.

Holiday shopping online is expected to reach new peaks this year, and with the surge comes concern over the safety of transactions, according to technology services company EDS Corp. and the U.S. Federal Trade Commission (FTC), both of which have issued guidelines for Web shoppers.

U.S. shoppers are expected to buy about 25% of their holiday goods online this year, with a typical shopper spending nearly $800, according to the National Retail Federation. With that in mind, various vendors and consumer groups have issued warnings for online shoppers because a likelihood of fraud accompanies the increase of buying online. Internet-related fraud cost an estimated $340 million last year, the FTC said.

According to EDS and the FTC, online shoppers should:

Know your retailer : Stick with reputable businesses with contact numbers and physical addresses. Some Web sites display seals that vouch for their security, but these can also be faked.

Use secure Web sites : Sites that use encryption to protect data should display "https://" rather than "http://" in the address bar. Secure sites should also display a padlock symbol to show that the Web site has a secure, encrypted connection. EDS advises against sending a retailer more information than they need to complete a purchase.

Be aware of phishing e-mail : Most people have received fraudulent e-mail asking for personal information. Never send information and never click on links in such e-mails, which are likely to be directed to look-alike Web sites designed to harvest identity and financial details. Reputable businesses do not ask for information through e-mails. However, it's safe to type a Web site address into a browser.

Review privacy and security policies : Most companies will tell you what information they collect and how they use it. Also, foreign Web sites may be bound by different laws for how they can handle your personal information.

Use antivirus and firewall software.

Check your credit report and credit card balances regularly.

Virtual Credit Card Numbers: Extra Safety or False Security for Online Shoppers?

By Sheryl Nance-Nash Posted 9:00AM 08/11/11 Technology, Bank of America, Citigroup, Credit, Retail, Personal Finance, Credit Cards

With all the hackers in the headlines -- the Sony PlayStation hacking fiasco (SNE) in April, then Tuesday's threat to "kill" Facebook -- you might be starting to feel a bit more hesitant to offer up your sacred credit-card digits online. One secret weapon, of sorts, aims to keep identity thieves at bay: virtual credit-card numbers.

Many major banks and credit institutions offer some version of this free service. Virtual credit card numbers aren't new, but they remain under the radar for many consumers. Are they the best-kept secret in online shopping, or is the security they promise just an illusion?

Here's what you need to know to decide for yourself:

How They Work

If your card issuer offers virtual credit-card numbers, all you have to do is log in to your account and follow the steps to generate a new virtual number each time you shop online.

After you apply -- and get approved -- for the program, you get an email with a virtual 16-digit card number and a virtual three-digit card-verification code that you can use in place of your bank-account or other credit-card number, says Michael Germanovsky, editor-in-chief of Credit-Land.com.

When you make a purchase, you simply use the newly generated number instead of your real account number. Each virtual account number is tied back to your actual credit-card account, so any transactions you make with the virtual numbers appear on your statement like all your other purchases, explains Beverly Harzog, credit-card expert for Credit.com.

The process varies slightly by issuer. But, generally speaking, you shop online as usual, except that you request a virtual number before checking out and use that number in place of the usual one. The virtual card numbers come with an expiration date, which -- in some cases -- you're able to choose. Some companies issue virtual numbers that can only be used once, while others allow the same number to be used multiple times at the same merchant, says Amber Stubbs, managing editor of CardRatings.com.

For a closer look at how these virtual numbers work, check out examples at Bank of America (BAC) , Citibank (C) and Discover Financial Services (DFS).

Peace of Mind -- for Free

Veteran consumer advocate Edgar Dworsky of Consumer World is a longtime fan of virtual credit-card numbers. "I use them in two situations, when dealing with an unfamiliar website and when I want to ensure that future charges -- such as a fee for another year of a particular service -- cannot be automatically charged to my card," Dworksy says. He always opts for the virtual card to expire in two months, which is the shortest period that Bank of America allows, and sets a limit no higher than the amount of the particular purchase.

"The best thing about virtual credit card numbers is that you can set the maximum credit limit, when it expires and what website it can be used on. They are useless to thieves. Well, that's the idea. But if they do get the number somehow, their actions are extremely limited -- almost impossible. In order for them to even attempt a transaction, they'd have to know where the credit-card number can be used. The purchase would also be declined if the transaction surpassed the set limit on the virtual number, and, of course, they could have long expired by the time they attempt to make a fraudulent purchase," says Howard Dvorkin, founder of Consolidated Credit.

Bob Williams, a senior vice president at a bank in Little Rock, shops online several times a week. He loves virtual credit-card numbers. "They allow me to shop online with total safety and protection of my primary credit-card number," he says. "I simply will not do business online with any other card because they don't offer this simple and safe methodology to transact business over the Internet."

For those who may not have sterling credit, no worries. "People with bad credit should know that these cards work much like any prepaid card. Good credit is not a necessity and there are no credit checks and no income verification to be had here," Germanovsky says.

Protection, but No Panacea

While virtual credit-card numbers are a great tactic to keep criminals from seeing your real account information, they aren't a panacea, Dvorkin says.

For one thing, they aren't 100% foolproof. Some customers have reported virtual-credit-card transactions that have gone through even when they've exceeded the limits the consumers have set, or when they take place well after the expiration date.

And, often, customers can only dispute statements for a limited time before they're responsible for the cost. "For people who don't pay too close attention to their credit-card statements, this could be a problem," Dvorkin says.

The bottom line is that you still need to carefully monitor your credit-card statements when you're using virtual numbers. "Virtual credit-card numbers offer an extra layer of protection, but they are not a cure-all," Stubbs says.

Nonvirtual Stumbling Blocks

The numbers can also raise stumbling blocks for customers, so it's important to think about how you use the phantom numbers. Rental-car companies, for example, want to see the card you used to reserve the car when you arrive to claim it. If you used a virtual number, it wouldn't match the number on your card, points out Linda Sherry, a spokeswoman for Consumer Action.

For additional protection, use the feature that lets you limit the amount charged. You might also want set your preferences so that all the virtual numbers are only good for one transaction unless you authorize a later expiration date, Williams advises.

Read the fine print and be aware of how long the number will be valid, particularly if you will be using the number for a recurring payment, Harzog says. Typically, the validity periods are short-lived, so if you use a virtual credit-card number to preorder products, the number could expire before the card is billed, Stubbs points out.

Know too, that these numbers can usually only be used online.

Virtual credit-card numbers have proven tricky for some business owners. " I've had some bad experiences, as a vendor, with virtual credit card numbers," says George Burke, founder and CEO of BookSwim.com, a Netflix-style book-rental service with monthly credit-card billing. "There have been instances where members have signed up with these virtual credit cards during a free trial and simply canceled that virtual number, resulting in us being unable to bill for the next month of service and them holding onto a hundred bucks worth of our inventory. We have had a pretty significant loss that was at first unexpected, but then had to be worked into our regular costs of doing business. Crazy right?"

Do You Need Double Protection?

Susan Grant, director of consumer protection for the Consumer Federation of America, isn't sure there's a compelling reason to get a virtual credit-card number. "There are strong credit card protections in place," she says. "You're only responsible for $50 if your card is stolen."

Then too, most major card issuers offer "zero liability" for online purchases. As Sherry says, "Most of the benefits are for the bank, which would be responsible for the charge if it was unauthorized or fraud."

But if you're a person who thinks safety means having both suspenders and a belt, then, yes, maybe virtual credit-card numbers are ideal for you.

Tips: Shopping Tip List

Here's a list of tips you should consult when shopping online. Print this page and keep it in a handy place so it will be easy to review before you order.

Trust your instincts. If you don't feel comfortable buying or bidding on an item over the web, or if you feel pressured to place your order immediately, maybe you shouldn't.

Be knowledgeable about web-based auctions. Take special care to familiarize yourself not only with the rules and policies of the auction site itself but with the legal terms (warranties, refund policy, etc.) of the seller's items that you wish to bid on.

Double check pricing. Be suspicious of prices that are too good to be true. Also consider carefully whether you may be paying too much for an item, particularly if you're bidding through an auction site. You may want to comparison shop, online or offline, before you buy. Make sure there are not extra shipping or handling costs.

Find and read the privacy policy. Read the privacy policy carefully to find out what information the seller is gathering from you, how the information will be used, and how you can stop the process. If a site does not have a privacy policy posted, you may not want to do business with it. If it does have a privacy policy, there will probably be a link to it from the seller's home page, or it could be included with the Legal Terms.

Review the return, refund, and shipping and handling policies as well as the other legal terms . If you can't find them, ask the seller through an e-mail or telephone call to indicate where they are on the site or to provide them to you in writing.

Make sure the Internet connection is secure. Before you give your payment information, check for indicators that security software is in place.

Use the safest way to pay on the Internet. Pay for your order using a credit card.

Print the terms. You should print out and date a copy of terms, conditions, warranties, item description, company information, even confirming e-mails, and save them with your records of your purchase.

Print the terms. You should print out and date a copy of terms, conditions, warranties, item description, company information, even confirming e-mails, and save them with your records of your purchase.

Insure the safe delivery of your item. If you're concerned you may not be home when your package is delivered and that someone may take it if it is left on the doorstep, ask whether you can specify that the shipper must receive a signature before leaving the package. Or, it may be safer to have the package delivered to your office.

Inspect your purchase. Look at your purchase carefully as soon as you receive it. Contact the seller as soon as possible if you discover a problem with it. Tell the seller in writing about any problems you have, ask for a repair or refund, and keep a copy of your correspondence.

Consumer Advice:

Consider opening a separate free checking account with just an ATM card and no checks. This account would act as an online purchasing account only and would be a way of controlling the amount of funds deposited and therefore avoiding significant loss if your account is illegally accessed. This account would be a stand-alone account with no connectivity to the main account. Transfer of funds could be made into this account for the specific online purchase amount. If fraud takes place, the loss would be minimal and the account could be closed with no hassle.