

A Consumer's Guide to E-Payments

The Internet has taken its place beside the telephone and television as an important part of people's lives. Consumers use the Internet to shop, bank and invest online. Most consumers use credit or debit cards to pay for online purchases, but other payment methods, like "e-wallets," are becoming more common. Luxury Spreads wants to make sure that you make an educated decision when using our online payment systems. If you have any additional concerns please investigate Luxury spreads by contacting our Suppliers Veratexinc.com or lawrencehome.com.

The Federal Trade Commission (FTC) wants you to know about these payment technologies and how to make your transactions as safe and secure as possible. Keep these tips in mind as other forms of electronic commerce, like mobile and wireless transactions, become more available.

And How Would You Like To Pay?

Most online shoppers use credit cards to pay for their online purchases. But debit cards - which authorize merchants to debit your bank account electronically - are increasing in use. Your debit card may be an automated teller machine (ATM) card that can be used for retail purchases. To complete a debit card transaction, you may have to use a personal identification number (PIN), some form of a signature or other identification, or a combination of these identifiers. Some cards have both credit and debit features: You select the payment option at the point-of-sale. But remember, although a debit card may look like a credit card, the money for debit purchases is transferred almost immediately from your bank account to the merchant's account. In addition, your liability limits for a lost or stolen debit card and unauthorized use are different from your liability if your credit card is lost, stolen or used without your authorization.

Other electronic payment systems - sometimes referred to as "electronic money" or "e-money" - also are now common. Their goal is to make purchasing simpler. For example, "stored-value" cards let you transfer cash value to a card. They're commonly used on public transportation, at colleges and universities, at gas stations, and for prepaid telephone use. Many retailers also sell stored-value cards in place of gift certificates. Some stored-value cards work offline, say, to buy a candy bar at a vending machine; others work online, for example, to buy an item from a website; some have both offline and online features. Some cards can be "reloaded" with additional value, at a cash machine; other cards are "disposable" - you throw them away after you use all their value. Some stored-value cards contain computer chips that make them "smart" cards: These cards may act like a credit card as well as a debit card, and also may contain stored value.

Some Internet-based payment systems allow value to be transmitted through computers, sometimes called "e-wallets." You can use "e-wallets" to make "micro payments" - very small online or offline payments for things like a magazine or fast food. When you buy something using your e-wallet, the balance on your online account decreases by that amount. "E-wallets" may work by using some form of stored value or by automatically accessing an account you've set up through a computer system connected to your credit or debit card account.

"Paying" It Safe

The FTC encourages you to take steps to make sure your transactions are secure and your personal information is protected. Although you can't control fraud or deception on the Internet, you can take action to recognize it, avoid it and report it. Here's how.

Use a secure browser - software that encrypts or scrambles the purchase information you send over the Internet - to help guard the security of your information as it is transmitted to a website. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting your purchase information, look for the "lock" icon on the browser's status bar, and the phrase "https" in the URL address for a website, to be sure your information is secure during transmission.

Check the site's privacy policy, before you provide any personal financial information to a website. In particular, determine how the information will be used or shared with others. Also check the site's statements about the security provided for your information. Some websites' disclosures are easier to find than others - look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If you're not comfortable with the policy, consider doing business elsewhere..

Keep your personal information private. Don't disclose your personal information - your address, telephone number, Social Security number, bank account number or e-mail address - unless you know

who's collecting the information, why they're collecting it and how they'll use it.

Give payment information only to businesses you know and trust, and only when and where it is appropriate - like an order form. Never give your password to anyone online, even your Internet service provider. Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.

Keep records of your online transactions and check your e-mail for contacts by merchants with whom you're doing business. Merchants may send you important information about your purchases.

Review your monthly credit card and bank statements for any errors or unauthorized purchases promptly and thoroughly. Notify your credit or debit card issuer immediately if your credit or debit card or checkbook is lost or stolen, or if you suspect someone is using your accounts without your permission.

Report Problems Immediately

The Fair Credit Billing Act (FCBA) and Electronic Fund Transfer Act (EFTA) establish protections against lost or stolen credit or debit cards, and procedures for resolving errors on credit and bank account statements that can include:

- credit charges or electronic fund transfers that you - or anyone you've authorized to use your account - have not made;
- credit charges or electronic fund transfers that are incorrectly identified or show the wrong amount or date;
- computation or similar errors;
- a failure to properly reflect payments or credits, or electronic fund transfers;
- not mailing or delivering credit billing statements to your current address, as long as that address was received by the creditor in writing at least 20 days before the billing period ended; and
- credit charges or electronic fund transfers for which you request an explanation or documentation, because of a possible error.

Billing errors: The FCBA's settlement procedures apply to disputes about "billing errors" for open-end accounts, including unauthorized charges (you cannot be liable for more than \$50 for unauthorized credit charges); charges for goods or services you didn't accept or weren't delivered as agreed; charges that are incorrectly identified or show the wrong amount or date; math errors; a failure to properly reflect payments or credits; not mailing or delivering credit billing statements to your current address, if the address was received by the creditor in writing at least 20 days before the billing period ended; and charges for which you request an explanation or documentation, because of a possible error.

To take advantage of the FCBA's consumer protections for errors on your account, write to the creditor at the address given for "billing inquiries," not the address for sending your payments. Include your name, address, account number and a description of the billing error. Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. And if you send your letter by certified mail, return receipt requested, you'll have proof that the creditor received it. Include copies (not originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your dispute in writing within 30 days after it is received, unless the problem is resolved within that period. The creditor must conduct an investigation and either correct the mistake or explain why the bill is believed to be correct, within two billing cycles (but not more than 90 days), unless the creditor provides a permanent credit instead. You may withhold payment of the amount in dispute and any related finance charges and the creditor may not take any action to collect that amount during the dispute.

How Not to Get Hooked by a 'Phishing' Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.

Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

Please visit the following sites for additional information on preventing internet credit fraud.

<http://www.antiphishing.org/>

<http://www.ifccfbi.gov/index.asp>

<http://www.cybercrime.gov/>

<http://www.business.gov/>

<http://www.firstgov.gov/>