

Common Frauds Phishing

“Phishing” is an email scam that attempts to trick consumers into revealing personal information, such as their credit or debit account numbers, checking account information, Social Security numbers, or banking account passwords through fake Web sites or in a reply email.

Phishing scams are among the fastest growing forms of fraud on the Internet. According to the Anti-Phishing Working Group, phishing scams grew by 52 percent from December 2003 to January 2004. Find out more about phishing below.

How to spot a phishing email

Phishing emails, and the Web sites they link to, typically use familiar logos and familiar graphics to deceive consumers into thinking the sender or Web site owner is a government agency or a company they know. Sometimes the phisher urges intended victims to “confirm” account information that has been “stolen” or “lost.” Other times the phisher entices victims to reveal personal information by telling them they have won a special prize or earned an exciting reward.

Look for these red flags in the email:

- Asks you to provide personal information such as your credit union account number, an account password, credit card number, PIN number, mother’s maiden name, or Social Security number. The Credit Union will never ask you for this information by email.
- Does not address you by your name.
- No confirmation of the company that does business with you, such as referencing a partial account number.
- Warns that your account will be shut down unless you reconfirm your financial information.
- Warns that you’ve been a victim of fraud.
- Spelling or grammatical errors.

Take these steps to minimize your phishing risk

View any email request for financial information or other personal data with suspicion.

Do not reply to the email and do not respond by clicking on a link within the email message.

Contact the actual business that allegedly sent the email to verify if it is genuine. Call a phone number or visit a Web site that you know to be legitimate, such as those provided on your monthly statements.

Do NOT send personal information (e.g., credit or debit card number, Social Security number, or PIN) in response to an email request from anyone or any entity.

Be cautious. Check your monthly statements to verify all transactions.

Forward any emails claiming to be from Visa or your Credit Union asking you to provide your personal account information to phishing@visa.com. You can also forward any suspicious email to the Better Business Bureau at nophishing@cbbb.bbb.org, and immediately call your Credit Union.

Identity Theft How It Happens

Identity theft can occur in a number of different ways. If you know what to look for and how it happens, you can self-detect identity theft before it happens, minimizing losses. Here are some common scenarios to watch out for:

What identity thieves can do

Using everyday items such as your driver's license or Social Security number to assume your identity, a skilled thief can:

- Open new bank accounts, and write bad checks.
- Establish new credit card accounts and not pay the bills
- Obtain personal or car loans.
- Get cash advances.
- Set up cellular phones or utility services and run up bills.
- Change your credit card mailing address and charge on your existing accounts.
- Obtain employment.
- Rent an apartment, but avoid the payments, and get evicted.

How identity thieves do it

Identity theft can occur in a number of different ways. But if you know what to look for and how it happens, you can minimize your overall risk. Here are some common scenarios to watch out for:

Lost/stolen wallet or checkbook

The most commonly reported source of information used to commit fraud is a lost or stolen wallet or checkbook. Stolen wallets and checkbooks usually contain a number of credit and debit cards, in addition to other personal documentation. Using these items, a thief can get enough information to obtain credit under the victim's name, or sell the information to an organized crime ring.

Dumpster diving

Thieves rummage through trash cans for pieces of non-shredded personal information that they can use or sell.

Definition: Dumpster Diving

Dumpster Diving (v.) When identity thieves rummage through dumpsters for personal information.

Mail theft

Crooks search mailboxes for pre-approved credit offers, bank statements, tax forms, or convenience checks. They also look for credit card payment envelopes that have been left for postal carrier pick-up.

Plastic Card Protection Basics

Stay safe by staying alert

Protecting yourself can be as simple as keeping your eyes and ears open. Here are some proactive steps to keep your financial information secure.

General Information

Do a regular review

You can catch unauthorized transactions early by checking your account details regularly — at least once a week.

Put alerts to work

Some financial institutions offer you the option to have "account alerts" delivered to your cell phone or email. This keeps you up-to-date and on top of any suspicious activity.

Get your credit report

It's your credit, so make sure no one else is using it. Check to ensure there aren't activities listed that you didn't initiate.

Card and PIN safety

Report lost or stolen cards immediately.

Sign your card on the signature panel as soon as you receive it.

Protect your cards as if they were cash.

Don't leave your credit cards in the glove compartment of your car. An alarmingly high proportion of all credit card thefts occur in glove compartments.

Never write down your PIN—memorize it. Also, never use your PIN as a password.

Ensure that you get your card back after every purchase.

Always check sales vouchers for the correct purchase amount before you sign them, and keep copies of your vouchers and ATM receipts.

Always check your billing statement and verify the amounts of your purchases.

Make a comprehensive list of all your cards and their numbers and store it in a safe place.

Don't volunteer any personal information when you use your credit card, other than by displaying personal ID as requested by a merchant.

Don't lend your card to anyone. You are responsible for its use. Some credit card misuse can be traced directly to family and friends.

Never disclose your PIN to anyone. No one from a financial institution, the police, or a merchant should ask for your PIN.

ATM safety

Using your Debit card at the ATM is a convenient and safe way to get cash. Just be sure to keep in mind the following safety tips:

Watch your surroundings

If the machine is poorly lit, or in a hidden area, use another ATM.

Guard your PIN

Keep a lookout for suspicious activity. Always guard your PIN and transaction amount, and immediately cancel your transaction and leave if you see something suspicious.

Keep your card ready

MORE

Zero Liability has you covered

It's simple. Shop online and off with absolutely no risk

Use your Credit Union Visa card to shop online, in a store, or anywhere, and you're protected from unauthorized use of your card or account information. With Visa's Zero Liability policy*, your liability for unauthorized transactions is \$0—you pay nothing.

Zero Liability has you covered

Worry-free shopping

Ultimate security

Complete fraud protection

Visa's Zero Liability policy means 100 percent protection for you. Visa's enhanced policy guarantees maximum protection against fraud. You now have complete liability protection for all of your card transactions that take place on the Visa system.

If you notice fraudulent activity on your card, promptly contact your credit union to report it. It is important to continually monitor your monthly statement to identify any unauthorized transactions.**

The Zero Liability policy covers all Visa credit and debit card transactions processed over the Visa network—online or off. The only transactions not covered under the Zero Liability policy are commercial card, ATM, and non-Visa-branded PIN transactions.

For transactions on other networks, the liability decision is left to the financial institution that issued your card. The issuer has the option of extending the same protections afforded by Visa's Zero Liability policy.

You're protected with Visa

Regardless of where you shop, enjoy the comfort of knowing you're protected with Visa.

*Covers U.S. issued cards only. Visa's Zero Liability Policy does not apply to commercial credit card, or ATM transactions, or PIN transactions not processed by Visa. Notify your financial institution immediately of any fraudulent use.

**Cardholders should always regularly check their monthly statements for transaction accuracy. Financial institutions may impose greater liability on the cardholder if the financial institution reasonably determines that the unauthorized transaction was caused by the gross negligence or fraudulent action of the cardholder—which may include your delay for an unreasonable time in reporting unauthorized transactions.

MORE

3-Digit Code

One more layer of security from your Credit Union and Visa

Also known as the Cardholder Verification Value or, CVV2, these three numbers help ensure that the physical card is in the cardholder's possession while shopping online or by phone, helping to prevent unauthorized or fraudulent use.

Where can I find it?

The 3-digit code is located on the back of your card, inside the signature area. Typically the signature panel will have a series of numbers, but only the last three digits make up the CVV2 code.



What does it do?

It's actually more about what it prevents. When shopping online or over the phone, the 3-digit code helps merchants ensure that the card is in the right hands. Merchants will request the CVV2 at checkout from the cardholder, and the information is sent electronically to the card-issuing financial institution to verify its validity. Within seconds, the CVV2 results are returned with authorization. If it's returned invalid, merchants have the right to stop the transaction.

And for your added protection, merchants are prohibited from keeping or storing the CVV2 number after the transaction has been completed.

MORE

Online Shopping Protection

Tips to keep you safe while shopping online

Shopping online can be fun and rewarding, but there are a few basic things you should know before you begin. Follow these tips to shop smart and stay safe.

Online shopping safety tips

Shop only at Internet merchants you know and trust; if in doubt, check with the [Better Business Bureau](#)

Beware of emails offering cut-rate prices on popular toys, software or other gifts; if the offer sounds too good to be true, it probably is.

If you receive an unsolicited email from an Internet merchant, do not click on the links within it. Instead, locate the merchant's Web site address through a reputable search engine or type the known address.

Check Internet merchants' refund policies; some merchants set a deadline for returns or charge a fee to accept returned merchandise.

Never share your passwords with anyone. Use different passwords for different Web sites.

Do not provide your social security number, birth date, or mother's maiden name in an email or within a Web site.

Ensure your computer has the latest anti-virus software installed before shopping online.

Always print and save the confirmation page when completing an online purchase.

Shop at trusted online retailers

You wouldn't shop at a brick-and-mortar store you didn't trust, so make sure you're as vigilant about your online retail choices. Buy from trusted sources, and if you're not sure do your research. Perform a background check, request a catalog by mail, or talk to a customer service representative for more information. You can also look for third-party seals of approval to get additional peace of mind.

Read return and shipping information

When calculating the final cost of a purchase, don't forget shipping and handling charges. If you're doing business with a merchant located in another state or country, taxes and international costs may apply. Before you buy, check the merchant site for a description of charges that will apply to your purchase.

Look for signs of security

Protect your private information while shopping online. Look for a padlock in the status bar at the bottom of the browser window, a URL that begins "https://", or the words "Secure Sockets Layer (SSL)." These signs indicate that only you and the merchant can view your payment information.