Member Education Center

Protect yourself by becoming informed about fraud and identity theft.
Fraudulent email (also called phishing, spoofing or imposter email) and fraudulent Web sites are used to trick people into providing personal information that can be used for identity theft.

Read a newspaper or watch the evening news and chances are there will be something about identity theft or other types of Internet fraud. As Internet usage has grown, so has Internet-related crime, especially fraud.

---

10 Tips For Accessing Your Accounts Safely Online

To help protect you against ID Theft as well as other Internet fraud, we have developed a checklist:

We recommend that you follow each of these steps to ensure you are taking the necessary safety precautions to protect your account information.

Since this will continue to be a growing issue of concern for consumers and the financial services industry alike, Huntingtonized FCU is taking aggressive steps to protect your information online. We've also developed a checklist to help you protect yourself.

We recommend that you implement each of these safety precautions to protect your account information.

1. **Update Your Online Banking Password.**
   This is perhaps the easiest precaution! Although changing your password is not required, we strongly recommend that you change it on a regular basis. This will help keep your accounts secure should someone obtain your user ID and password. Choose passwords that are not obvious and that would be difficult to guess. To strengthen security, choose a password consisting of both alphabetic and numeric characters. And remember – never share your password with anyone else.

   To change your password:

   Log in to CU Click.
   Select Change Password tab.
   Follow the remaining instructions to change your password.

2. **Security Phrase.**
   You can keep your Online Banking accounts more secure every time you logon.

   If you recognize your Security Phrase, you'll know for sure that you are at the valid Huntingtonized FCU site. Confirming your Security Phrase is also how you'll know that it's safe to enter your Password.
   If you feel that the information may be inaccurate, please call us immediately at 304-528-2400 weekdays, 8:00 a.m. to 4:00 p.m. ET.

3. **Don't Open Links In Emails.**
   Hackers frequently try to get information from individuals by sending emails asking for verification of account information. These deceptive emails may say that your bank account has been closed due to fraudulent activity or that it needs to be verified. If you ever receive an email of this nature, do not open the attached files, and do not provide any personal information. Huntingtonized FCU will never solicit your personal or account information through email.

   If you receive any email – from Huntingtonized FCU or from anyone else – requesting personal or account information, please treat it as fraudulent and forward it to us at hfcu@huntingtonized.com

Or, you can call us at 304-528-2400 weekdays, 8:00 a.m. to 6:00 p.m.

4. **Install A Firewall.**
   A firewall is your computer's first line of defense, because it protects your machine from hackers and intruders. A firewall is a software program that guards the entrance to your private network and keeps out unauthorized or unwanted traffic. It acts as a buffer between your computer and the outside world, allowing you to determine what traffic may access your computer. You can purchase a firewall program from your local computer store.

   Most firewall programs allow you to set the level of security protection that you desire. A good rule of thumb is to start with the highest protection setting and then relax the settings as necessary. The price of a firewall program starts at about $40 and includes features such as email attachment protection, advertisement blocking, pop-up-window protection and other automatic functions.

5. **Use Anti-Virus Software.**
   Anti-virus software protects your computer against viruses – unauthorized computer codes that attach to a program or portions of a computer system. Viruses reproduce and spread from one computer to another, destroying stored information and interrupting operations. An anti-virus program detects and destroys these unauthorized codes. With new viruses emerging daily, you need to have your anti-virus program updated regularly. Software manufacturers often sell their anti-virus programs with their firewall as a package, since they're natural complements.

6. **Use Anti-Spyware Software.**
   Spyware is any software program that aids in gathering information electronically about people or organizations without their knowledge or consent. It then relays that information to an unauthorized third party. Users most often open the door to spyware unwittingly by downloading free software indiscriminately or by clicking on pop-ups or dialogue boxes.

   Some kinds of spyware will redirect your browser to a new home page (not of your choosing). Others generate multiple pop-up ads that can make web surfing a chore. Another type of spyware known as a "keystroke logger" can cause the most damage, because this type of program records a copy of each character you type (such as user names and passwords to secure web sites) and sends that information to an unauthorized party who can steal your personal information. Among the anti-spyware programs on the market today, some are free, but most cost about $25.

7. **Read Your User Licensing Agreements.**
   It's possible for you to inadvertently agree to accept spyware with a program you're downloading. So be sure to thoroughly read any agreement included with applications or software you're about to download. Complete the download only if you recognize the additional programs included and you know they are safe. Always deal with reliable sources – products or companies you know or that are recommended by others you trust.

8. **Examine Browser Security Settings.**
   Make sure the security settings in your browser (Internet Explorer, for example) are set to provide an appropriate level of protection. Browser-based attacks can occur when a user visits a web page containing hidden code intended to sabotage a computer or compromise one's privacy. Use the Help feature of your Internet browser program to familiarize yourself with the security features available for your particular browser, or visit the browser manufacturer's web site for more information.

   To edit your security settings for Internet Explorer:

   Click on Tools on the menu bar.
   Select Internet Options from the pull-down menu.
   Click on Security.

9. **Take Advantage Of Security Updates.**
   Your Internet service provider (AOL, for example) and your Internet browser software manufacturer (for example, Microsoft) periodically issue security updates. These updates are often created to patch holes that allow viruses to get through. Many reputable software manufacturers dedicate sections of their web sites to security updates of this kind. If you don't have or don't use auto-

update mechanisms in your software, it's a good idea to visit the manufacturers' websites regularly to make sure you have the latest fixes.

10. **Use A Computer That Is Secured At All Times, Even When You're Traveling.**
    Even if you follow all the steps outlined here for your home computer, none of it will matter if you use a different computer that isn't secured. Be especially aware of this if you are traveling, for instance, or whenever you're using a work or personal computer that you typically don't use. If you must use a computer other than your own, first make sure that it has all of the items on this checklist installed and updated on its system.

    For the same reasons, it is also a good rule of thumb to avoid letting unfamiliar people have access to your computer. And, whenever you're not using the Internet, we recommend disconnecting your Internet access.

Some Things You Can Do If You Are A Victim Of Identity Theft

Following are some options that may be helpful if you are a victim of identity theft.

1. **Contact Us:**
   If you are a victim of identity theft with respect to any of your accounts or transactions with us, please notify us at:

   Huntingtonized FCU

   304-528-2400 (HTGN) 304-528-3400 (WAYNE) 304-716-9159 (MILTON)

   Please provide as much detail as possible about the accounts or transactions in question, including any dates and account or transaction numbers that apply. We will contact you to discuss additional information necessary to resolve the matter.

2. **Contact One Of The Major Credit Reporting Companies:**

   Equifax.....1-888-766-0008
   Experian.....1-888-397-3742
   TransUnion.....1-800-680-7289

   If you call one of these companies, they will pass on your information to the other two companies, saving you time. Each company will follow a standardized three-step process to post a security alert on the credit file, opt you out of pre-approved offers of credit or insurance and mail you a copy of your file.

   Here is what the process will look like in more detail once you make the call:

   - The company receiving the initial call will notify you of the ID fraud initiative and will electronically notify the other two credit reporting companies of the crime.
   - A fraud alert will be put on your credit report at all three nationwide credit reporting companies within 24 hours.
   - You will be opted out of all pre-approved offers of credit and insurance for two years.
   - Your request for a copy of your credit report will be handled in no more than three business days. Each of the three national credit reporting companies will work with you to verify the information in their respective reports and to delete any fraudulent data. If you file a police report, the process is even quicker. The Consumer Data Industry Association's national credit reporting company members will voluntarily expedite services for you by immediately deleting fraudulent data without the usual reinvestigation procedure.

- The fraud alert will be displayed by each national credit reporting agency to all lenders or other users that access the reports in the future.

3. **Report The Crime To Your Local Police & Sheriff's Departments.**
   Even if the police can't catch the identity thief, having a police report can help you in clearing up your credit records later on. Get a copy of your police report. You may need to provide a copy of the police report to the creditors.

4. **File A Complaint With The Federal Trade Commission (FTC)**
   File a complaint with the Federal Trade Commission (FTC) at **www.consumer.gov/idtheft** or call their toll-free hotline 1-877-IDTHEFT (438-4338).

5. **If Required, Fill Out An Identity Theft Affidavit.**
   Credit Unions, Banks, credit reporting agencies and other credit grantors may require you to complete an identity theft affidavit or other forms. Ask each credit union, bank or agency for its specific requirements.

6. **Notify Your Local Postal Inspector Of A Fraudulent Change Of Address.**
   Notify your local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit credit or bank fraud. (Call your local Postmaster to obtain the phone number.) Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address.

RESOURCES			
FTC **www.consumer.gov** 1-877-IDTHEFT (438-4338)	**Equifax** **Equifax** 1-888-766-0008	**Experian** **Experian** 1-888-397-3742	**TransUnion** **TransUnion** 1-800-680-7289

How To Recognize Fraudulent Email

Be wary of any seemingly legitimate email request for account information, often under the guise of asking you to verify or reconfirm confidential personal information such as account number, Social Security Numbers, passwords or other sensitive information.

It's often hard to detect a fraudulent email. That's because the email address of the sender often seems genuine (such as support@yourbank.com), as do the design and graphics. But there are clear signs to be aware of. For example, fraudulent emails often try to extract personal information from you in one of two ways:

By luring you into providing it on the spot (e.g., by replying to the email), or

Including links to a Web site that tries to get you to disclose personal data

Like the email, a fraudulent Web site is designed to trick you into believing it belongs to a company you know by using its brands as domain names and/or its graphics. The ultimate goal of this fraud is to use your information to gain unauthorized access to your bank or financial accounts or to engage in other illegal acts.

Do not reply to any email requesting your personal information, or one that sends you personal information and asks you to update or confirm it. If you receive an email you are suspicious of, contact the company through an address or telephone number you know to be genuine. HUNTINGTONIZED FCU will never send you any email that requests your account information or asks you to verify a statement.

If you suspect you have provided confidential account or personal information to a fraudulent Web site, change your password immediately, monitor your account activity frequently and report any suspicious activity to the company.

What You Can Do About Phishing Schemes

The Department of Justice recommends following three simple rules when you see emails or Web sites that may be part of a phishing scheme: **Stop, Look, & Call**.

Stop. Phishers typically include upsetting or exciting (but false) statements in their emails with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Resist that impulse to click immediately. No matter how upsetting or exciting the statements in the email may be, there is always enough time to check out the information more closely.

Look. Look more closely at the claims made in the email, think about whether those claims make sense, and be highly suspicious if the email asks for numerous items of your personal information such as account numbers, usernames, or passwords. For example:

If the email indicates that it comes from a bank or other financial institution where you have a bank or credit card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate banks and financial institutions already have their customers' account numbers in their records. Even if the email says a customer's account is being terminated, the real bank or financial institution will still have that customer's account number and identifying information.

If the email says that you have won a prize or are entitled to receive some special "deal," but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize don’t ask you for extensive amounts of personal and financial information before you're entitled to receive it.

Call. If the email or Web site purports to be from a legitimate company or financial institution, call or email that company directly and ask whether the email or Web site is really from that company. To be sure that you are contacting the real company or institution where you have accounts, credit card accountholders can call the toll-free customer numbers on the backs of your cards, and bank customers can call the telephone numbers on your bank statements