HARTFORD HEALTHCARE FEDERAL CREDIT UNION

Cyber Security & Fraud Suggestions

Did you know criminals have stolen over $3.1 billion dollars from October 2013, to June 2016, using hacked email and bank accounts to preform wire transfers and online bill payments?(*) Review this checklist regularly to help ensure you're following cyber security & fraud best practices to further protect your identity and bank accounts.

Protect Your Password

- Never share your account name and passwords
- Use a strong password of at least eight (8) characters, using a combination of upper case, lower case, numbers and special characters (i.e., H@1h*C0u).
- Ensure your password is stored securely (e.g., locked drawer, encrypted mobile application etc.).
- Never save your user name and password on websites that store sensitive and/or financial data (e.g., debit/credit card number and expiration data, billing address, etc.).
- Do not re-use your passwords on multiple websites as malicious individuals will attempt use a stolen user credentials on various websites (e.g., email, banking, online stores, etc.).
- Enable *"multi-factor authentication"* if offered by the website as it drastically decreases the potential for a malicious individual to access your account.

Protect Your Computer

- Do not open attachments or hyperlinks from suspicious emails that you were not expecting.
- Avoid downloading files from unfamiliar file sharing sites as they may contain malware.
- Perform file backups on a regular basis to avoid losing files due to a malware infection.
- Update your operating system with patches on a regular basis.
- Ensure you have an anti-virus program installed on your computer with updates being performed daily and scans running regularly.

Protect Your Mobile Phone

- Enable security settings that requires a passcode to be entered after a period of inactivity.
- Update your mobile operating system with upgraded versions in a timely manner.
- Avoid installing applications from unofficial third-party marketplaces.
- Read privacy policies to see how the application creator will be using your personal information (e.g., geo-location, phone contacts, social media posts, photos/videos, etc.).

Online Shopping

- Before shopping online, make sure that the website uses secure technology, such as a website using https instead of http.
- Always be cautious about shopping online when using a wireless public network as you don't know if the information you are transmitting can be intercepted.
- While convenient for future purchases, avoid storing your debit card/credit card number when asked by websites.

Social Media

- Consider making your social media profiles "private" to help prevent malicious individuals from attempting to gain information that they can use in an attempt to reset passwords (e.g., mother's maiden name, birthdate, name of middle school, etc.).
- Only accept social media connection requests from people you know.
- Avoid clicking on hyperlinks on suspicious posts as malicious individuals use this method to try and steal your personal information.

Fraud & Scams

Common scams to look out for include:

- Fraudulent Mobile Check Deposit - "Deposit this check and send us some of the money back or get a reward..."
- Lottery/Sweepstakes – "You won the lottery, wire us money for misc. fees…"
- Fake Credit Union Text or Phone Call – "This is your Credit Union, please confirm your information…"
- Online Love Interest – "Send me money to come visit/stay with you…"

Prevent yourself from becoming a victim of scams that target your Credit Union account. We want to remind you that **you should never share your Online Banking or Mobile App User ID and/or Password with anyone.** In doing so, you expose yourself to significant risk.

Remember, **legitimate financial companies will not contact you asking for account numbers or personal information.** When in doubt, get in touch with your institution directly using contact information that you have verified yourself.

Do you have questions about Cyber Security & Fraud?

Click here for FBI information on Scams & Safety.

https://www.fbi.gov/scams-and-safety/common-fraud-schemes

We're happy to help. Please email Eric at ericb@hhcu.org

**FBI Public Service Announcement (I-061416-PSA) – October 3, 2016*

"We care for you as you care for others."