Protect Yourself

From Identify Thieves and Fraud Scams.

Protection tips and suggestions compiled by Redbrand Credit Union February, 2017.

Electronic Device Protection

- Screen Lock your device when not in use (cell phone, tablet, PC).
- Create strong passwords; ones that are different from your name, username, address, D.O.B., made up of letters (upper and lower case) and numbers and include at least one special character (!@#$%^&*).
- Do not store your passwords or other confidential information on your computer, phone or in an app. If you must write down your passwords, store them in a secure location.
- Do not share your passwords with anyone.
- Do not access secure sites while on a public Wi-Fi network (e.g. Coffee Shop or Travel Stop).
- Do not "jail break" your mobile device. This may make your device vulnerable to malicious software.
- Wipe your device before discarding or selling it.
- Redbrand CU will not contact you via TXT message. Do not respond to any txt message claiming to be Redbrand or another similar institution.

Personal Protection

- Reconcile accounts monthly using your transaction register.
- At a minimum, review your credit report annually. Everyone is entitled to a free copy of their credit report 1x per year from each of the credit reporting agencies. Visit www.annualcreditreport.com (link on www.redbrandcu.com) or visit each of the agencies individually: TransUnion, Equifax and Experian. Want to be extra vigilant? Request a free copy from one of the three agencies every 4 months.
- Do not share personal/confidential information with people you have not met in person.
- Do not take Facebook, or other relationships on social media, to be the person portrayed; even if you have met the person.
- Do not send money to someone unless you are 100% certain of their identity and that the funds are being used legitimately.
- Do not accept a check/payment from someone for which they have over paid. If you do, do not send any money back without talking to a teller or law enforcement officer first.

Card Security

- Activate your cards as soon as you receive them. Destroy old cards immediately.
- Immediately enroll your card in Verified by Visa. Search "Enroll Verified by VISA" in your search engine to get started.
- If you write down your PIN numbers, keep them in a secure place separate from your cards. DO NOT keep them in your wallet/purse/car or anywhere near the card.
- Do not use personal information for your PIN number (e.g. SSN, address, information in wallet) or common PINs (e.g. 0000, 9999, 1234, 2580…).
- DO NOT give your card or PIN to anyone not authorized on your account.
- When entering your PIN, (at the ATM or store) block your entry so your PIN can not be captured by someone looking over your shoulder.
- Report a lost card immediately: (309) 697-1447.
- Avoid going to the ATM at night, especially walk-up locations.
- Pay attention to the slot in which you insert your card. If there appear to be "extra" or loose pieces, do not proceed and contact the financial institution immediately.

Online Protection

- Shop only on secure sites (padlock icon displays on URL bar and https://).
- Always log off of secure websites as soon as you are done.
- Review all fine print carefully, especially when entering your card information online, to avoid unexpected charges.
- Only download programs from known sources, such as the Play/App Stores.
- Keep security patches, anti-virus and malware software, browser versions, and plug-ins up to date for your devices.
- Configure your devices to prevent unauthorized users from remotely accessing your devices or home network.
- Do not save financial/confidential documents online (Cloud Storage) until you have read the company's security and privacy policy and have verified that the site is secure and information is encrypted (password protected/https://).
- Keep information on social media sites minimal. Do not post information that may be used by financial institutions and other businesses as means of identification.

Email Security

- Redbrand Credit Union, like most entities, will not contact you via email and ask for confidential information. Do not reply to emails or other communications requesting you to enter information. If you are unsure about the email or communication, contact the sender using information that you already have, or that is publicly available.
- Do not open attachments from unknown sources, or even attachments from known sources that you weren't expecting.

Lottery Scam

Mrs. Smith, currently retired, worked 35 years. She is enjoying her hard earned pension and also has a nice little "nest egg" saved. Mrs. Smith gets an email one day, claiming that she won the lottery! "Bonus!" she thinks. She follows the link, and reads the details, but doesn't catch that this is the *Canadian Lottery...* nor that she has never played before.

She goes on to read that in order to claim her winnings, she must first pay a "tax" or "fees" in the form of a money order, cashier's check, western union or wire (all certified funds). It all looks very official, so she goes ahead and sends the money off... only to hear back that they need additional fees before the payout can happen.

Mrs. Smith was always sharp as a tack, but since retirement isn't quite as sharp as she used to be. Many people figure out this scam quickly, but Mrs. Smith doesn't. Despite the warnings of multiple employees of the CU, other financial institutions and even law enforcement, she continues to send money. The people talking to her on the phone have "become her friends" and she looks forward to their conversations, and believes them firmly.

The total amount Mrs. Smith lost is uncertain, because funds were sent from multiple sources, however it is believed to be at least $200,000. Law Enforcement was involved, but was not able to do anything as cyber criminals, especially those overseas, are very difficult to locate.

Grandson In Jail Scam

Mr. Gray received the phone call no Grandparent wants to get. His Grandson, Joey, was calling from Mexico, where he was being detained for an incident involving a car accident. Joey is scared to death and needs money ASAP to lessen the consequence of his crime.

Mr. Gray comes down the Credit Union to send the money. Credit Union employees are trained to be especially vigilant with foreign transactions. He persists that this is not a scam and that he *actually* spoke with his Grandson. The CU sends the money, $1,000.

Mr. Gray comes back down later in the day. His Grandson called him back. He hit a light pole in the accident and needs more money to get out of jail and get home. He needs another $3,000. At this point the CU is especially suspicious. We ask if we can call the Grandson at home, which is in Arizona. We call... Joey answers. He's at work. In Arizona.

Mr. Gray actually believed he spoke with his Grandson. It is highly recommended that additional verifications , such as calling other family members to verify travel plans, be made before reacting to these types of situations.

***Names and identities have been changed to respect the privacy of our members.**

Romance Scam

Mrs. Brown, recently widowed, has been very lonely and "lost" since losing her husband almost a year ago. An old acquaintance, a friend of her husband's even, reaches out to her on Facebook. They immediately strike up a relationship and he informs her that "Mr. Brown wanted him to take care of her." She's overcome by the news and will do anything for him. Even send him money.

The story is that he's a Captain in the military, stationed in Afghanistan. He owes a friend some money, and has to take care of this in order to come home. She comes into the Credit Union, requesting a wire be sent to Nigeria. At this point both the Credit Union and Law Enforcement had to work hard to convince Mrs. Brown this was fraud.

Thankfully, with the help of the FBI, the plot came full circle. She was instructed to cease any and all communication with the "boyfriend," who was really a team of hackers that took over Mrs. Brown's deceased husband's friend's Face Book page. *Other members have not been so lucky, many have lost hundreds of thousands dollars to this scam.*

These con artists particularly target the recently widowed. It is highly recommended that the recently widowed keep a strong support system, and keep open and honest communication about what's going on with the members of that support system.

Grandson Borrows Debit Card

Mr. Johnson has invited the grandkids over for the weekend. At dinnertime, he realizes he forgot something at the grocery store. He hands his debit card to his 17 year old grandson and asks him to run to the store fast. No big deal, right?

Wrong. The grandson runs to the store and makes the purchase... even giving the card back to Grandpa right away. But when balancing his checkbook at the end of the month, Grandpa finds unauthorized charges from gaming companies. He doesn't play video games, these definitely are not his.

Further investigation reveals that the grandson made the purchases via his gaming system with the card information he had written down off of grandpa's card.

Luckily, in this case, the merchant refunded Mr. Johnson the charges and he got his money back.

***Names and identities have been changed to respect the privacy of our members.**