PREVENTING ACCOUNT FRAUD

Burns & McDonnell Credit Union takes the privacy of our clients and the security of their accounts very seriously. Currently, there are a number of e-mail scams that are designed to trick you into providing your user ID and password.

To help you defend yourself against these criminals, Burns & McDonnell Credit Union has compiled a list of simple online tips to help you safeguard your accounts and privacy from these online scams. We've also provided you with some general information on how to prevent account fraud and included links to the FTC's and NCUA's web pages that contain more detailed information about online safety, identity theft and online fraud.

How Financial Institutions will and will not contact you.

Financial institutions (FIs) and the Internet: two things that seem to work together so beautifully. How simple is it to check your balance or pay a bill online these days?

At the same time, phishers have used this fact to commit millions of dollars' worth of fraud and identity theft over the past decade. Is there a general rule to be derived here?

You can't just say "never trust an email or a text from a financial institution," because credit unions, banks and credit card companies definitely use email. Many people these days get their bills through email, and have stopped receiving paper statements years ago. Many FIs also offer services for mobile phones, from text message alerts to mobile banking applications for smart phones.

So how do you tell the difference between a real email and a phishing attack?

If an email or text message from a financial institution asks you to click a link to login and "verify" or "reactivate your account," it is a phishing attack. Delete the message immediately.

When you open an account, your FI is required to get your personal information. They check this information against national databases to verify it. Once an account is open, they've got your information. There is no need to have you verify it online. Any verification is already complete.

Sometimes card companies may contact you regarding unusual activity on your card. This is a security feature. However, they also never ask you to verify personal information.

You may receive a call if suspicious activity occurs with your credit or debit card. An automated message will give the name of the card stating there has been some unusual activity. If you know where the card is, it says to press "1." At no point will you have to verify personal information.

Of course, this also illustrates how important it is to keep your phone number, mailing address and other contact information current with any FI you have a relationship with.

Finally, if you're unsure whether or not an email message might be genuine, the way to find out is *not* to click on that link. Call your FI directly, using either a number from their actual website or by looking in an old fashioned phone book.

Online Security
Burns & McDonnell Credit Union takes online security of our members' accounts very seriously. Currently, there are a number of e-mail scams that are designed to trick you into providing your user ID and password. We will never request this information from you via e-mail. Here are some important Online Security tips:

- Keep the security features of your computer software up-to-date. This includes your Web browser, virus scan software and firewall. E-mail attachments and links within email can sometimes contain viruses and infect your computer without you knowing. Running frequent scans for viruses is highly recommended.

- Don't respond to unsolicited e-mails from companies that you do business with requesting that you re-validate your personal information or that provide a link to Web sites that require you to revalidate your account information. These links often lead to bogus web sites that look legitimate in order to fool you into providing secure information.
- Before entering personal information on any web site, look for the "locked padlock" icon in the browser frame, or "https" at the beginning of the web address to ensure that the site is secure.
- Change passwords regularly.
- Log off of the Web site after you have submitted an application or concluded a secure online session.
- When your computer is not in use, shut it down or disconnect from the Internet.
- If you think you may have fallen victim to an online scam, change your passwords and monitor your account activity closely.

Encrypted Information
Encryption helps protect your private information by scrambling it so that it cannot be intercepted and read by anyone else. When you visit a site that requires encryption, your browser will display a key or a lock. If you are not in a secure area, the key or lock will be broken.

For Microsoft browsers: To check your level of encryption, go to the "File" menu, select "Properties", and then select "Security." Another way is to select "Help" then "About Internet Explorer."

Other Security Features
Our firewall protects Burns & McDonnell Credit Union' systems by allowing entry only to those who are authorized.

For digital identity verification, the Online Banking system has a digital server certificate by VeriSign that your browser uses each time you sign on to verify that indeed you are connected to Burns & McDonnell Credit Union' Online Banking.

Your Role In Security
While Burns & McDonnell Credit Union works to protect your accounts, you also have a part. There are a number of steps you can take to ensure that your online experience on the Internet is safe and secure.
Most importantly, don't reveal your online Personal Identification Number to anyone. Your online PIN is designed to protect the privacy of your online information, but it will only work if you keep it private. If you think your online PIN has been compromised, change it immediately online.

- Don't leave your computer unattended if you are in the middle of an Online Banking session.
- Once you have finished your Online Banking session, always sign off before visiting other sites on the Internet.
- If anyone else is likely to use your computer, clear your browser cache or turn off your browser and re-start it in order to eliminate copies of web pages that have been stored on your hard drive. How you clear your cache will depend on the browser and version you have. This function is generally found in the browser's preferences menu.
- Burns & McDonnell Credit Union recommends that you use a browser with 128-bit encryption.

What is a "Phishing" scam?
"Phishing" is an e-mail scam that attempts to trick consumers into revealing personal information - such as their credit or debit card account numbers, checking account information, Social Security numbers, or banking account passwords - through fake Web sites or in a reply e-mail. Typically the e-mails and Web sites use familiar logos and slick 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.

Spotting a Phish
While phishing e-mails can be quite sophisticated in appearance, the following features are often indicators. An e-mail could be a scam if it:

- Asks you to provide personal information such as your bank account number, an account password, credit card number, PIN number, mother's maiden name, or Social Security number.
- Fails to address you by your name.
- Warns that your account will be shut down unless you reconfirm your financial information.
- Warns that you have been the victim of fraud.
- Has spelling or grammatical errors.

How to Stay Safe Online
Keep the security features of your computer software up-to-date. This includes your Web browser, virus scan software and firewall.

- Be cautious. View any e-mail request for financial information or other personal data with suspicion. Do not reply to the e-mail and do not respond by clicking on a link within the e-mail message.
- Don't open e-mails or attachments from unknown sources. Be suspicious of any unexpected e-mail attachments even if they appear to be from someone you know.
- Go directly to the company website by opening a new browser window and type the web address.
- Contact the actual business that allegedly sent the e-mail 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, online passwords or PIN) in response to an e-mail request from anyone or any entity.
- Review your statements. Check your monthly statements to verify all transactions.
- Always log off the web site after you have submitted an application or concluded a secure online session (such as Online Banking).
- Be careful and selective before providing your e-mail address to a questionable Web site. Providing your e-mail address makes you more likely to receive fraudulent e-mails.

Remember, Burns & McDonnell Credit Union will never ask you for personal information via e-mail.

If you suspect you have received a fraudulent e-mail that appears to be from Burns & McDonnell Credit Union, please forward it to us immediately at memberservice@bmcdcu.com. If you have specific questions related to fraud or have any other bank related questions, please call us at 816-822-3189. We appreciate your help in our effort to fight e-mail and online fraud. Know that Burns & McDonnell Credit Union takes preventing fraud for our clients and the security of their accounts very seriously.

For more information about protecting yourself online, "phishing" scams and identity theft, visit:

http://www.fdic.gov/bank/individual/online/safe.html
http://onguardonline.gov/phishing.html
http://www.consumer.gov/idtheft