Fraud Awareness

MCU takes your security seriously. Let's look at what we do to keep you secure. And what you can do, too.

Contents

Click any title to view the section instantly.

[Design box for following copy:]

Top Tip! Think your MCU accounts have been compromised? Call the Contact Center at **1-844-628-6969.**

"S" for Security

The first step in online security is checking for the lock icon and the letters **https://** at the beginning of the URL in your web browser (the webpage address at the top left of your page). The letter "s" in "https" means that your connection is secure.

At MCU we employ the highest standards of security to protect your account info against Identity Theft and Fraud, including:

128-bit Secure Socket Layer (SSL) technology to encrypt your personal information, making it scrambled when transmitted over the internet, only to be decoded upon reaching your secure browser.

What We Do

MCU Online Banking requires the use of a browser that supports 128-bit encryption. Members access their online accounts by enrolling in **NYMCU Online Banking** and automatically starting their financial journey with robust online security.

Let's say, as one example, that you're making an online loan application with MCU. All loan applications are secure and encrypted, protected by multi-level data security.

[Design box for following copy:]

Top Tip! As of June 2022, Microsoft no longer supports the browser Internet Explorer. We strongly recommend that IE users download Microsoft Edge.

What We Don't Do

MCU will **never contact you by email, text message or telephone** to ask you to update or verify your account information.

During your online banking login process, we will **never ask you to further verify** your login by inputting credit card or account information.

DO NOT respond to unsolicited text messages, email messages or telephone call asking for any account information or other private info. If you think your MCU accounts have been compromised, call the Contact Center at **1-844-628-6969.**

Dos & Don'ts for You

Password Strength is one of the top defenses against banking and identity fraud. When you create your password in NYMCU Online Banking, our system will rate its strength to help you create a password that is extremely hard for third-parties to guess. Other password security measures for you are:

1. **Don't** share your password with anybody, for any reason.
2. **Don't** write your password down or leave it laying around.
3. **Don't** reuse old passwords from old accounts.
4. **Don't** use the same passwords for current accounts.
5. **Do** change your password regularly (and set a reminder so you'll do it).
6. **Do** answer security questions with answers others don't know.
7. **Do** use two-factor authentication, so you can confirm on a separate device.
8. **Do** check any third-party access you granted and be strict about removing.

And like your password, file your **ATM PIN, online banking username** and **account info** under **TOP SECRET.** Don't share them, or leave them written down and/or lying around.

[Design box for following copy:]

Top Tip! Set up Account Alerts through NYMCU Online Banking and spot anything suspicious. Email or text messages will alert you when certain activity takes place.

What You *Should* Share

Planning a trip? We'd love to hear about it if you'll be using your **MCU ATM/Debit card** or **Visa credit card**. Sudden changes in your spending habits or patterns can trigger a security alert.

This is especially true if you're traveling outside the state or country.

For your protection, most foreign countries are blocked. If potential fraud is detected, your card may be temporarily suspended until any questionable charge is verified.

If you're out of town our attempts to protect you could frustrate you. Let's avoid that. With your place of travel and departure/return dates on hand, you can contact us securely and simply as follows:

Online Banking:

- Log in to NYMCU Online Banking.
- Click the "More" widget.
- Click "Message Center".
- Send a secure message with your details.

Alternatively, you can call the **Contact Center at 1-844-628-6969,** or visit your nearest branch and speak with a **Member Service Representative**.

Scams to Watch Out For

There are many ways that unscrupulous groups or individuals can gain access to your personal information, or your company information, through you. Here we'll look at some of the top tricks that are used, often successfully, and help you to spot them, avoid them, and report them by referring to our Reporting Suspected Scams section at the bottom of this page.

Social Engineering Scams

Think charming con-artist. Social engineering happens when an individual poses as a trustworthy person and gains your time and trust. The goal is usually to obtain or compromise information about an organization or its computer systems.

This person may claim to be a new employee, researcher, repair person, or essentially anybody likely to approach you and ask for help. This person will often offer some type of "identification" to win you over. Any information given to such a person will be collected and used to aid their ultimate goal.

If the individual moves from you to somebody you recommend, your name and position would be used to gain the trust of the next victim in the chain.

Below are detailed variations of this type of scam.

Phishing Scams

The heart of the phishing attack is the appearance of trustworthiness. It comes in the form of an email or website, which appears to represent a trustworthy individual, or an organization. Appearance is everything here and it's increasingly difficult to spot a fake based on that alone.

You may receive an email from, for example, a "credit card company" alerting you to a problem and asking you to confirm sensitive account information. Or you could be approached by a "charity," especially after a disaster or heavily highlighted issue in the news media.

You may even receive an email from a "friend or colleague" you trust, making it even more difficult to avoid downloading attached documents or using a link to a site from the body of the email.

Spoofing Scams

Spoofing is a type of fraud where a scammer contacts a person through phone, email, text or fax and pretends to be from a trusted source. The phone number, email address or website URL the scammer is using is disguised to look like an official communication from the organization they are pretending to be representing.

The scammer is trying to get the recipient to provide them with confidential data like passwords, account information, social security numbers, etc.

Vishing Scams

Vishing means a con enacted using voice communications. The name comes from "Voice Phishing". Like phishing and social engineering, you are contacted by somebody who seems trustworthy. In some cases, Voice over Internet Protocol (VoIP) solutions and broadcasting services are used (or abused).

This can enable a scammer to easily spoof caller ID, thus creating trust. Defenses are often down due to trust in phone services, especially landline. In most cases, the victim receives a call from a voice message claiming to represent a financial institution.

Victims have been asked to call a number provided and enter their PIN or account information. In some cases, people claiming to be calling from Apple or Windows have informed victims that immediate action must be taken to avoid being hacked!

Smishing Scams

Smishing is phishing by text. Once again, a text message is sent from what appears to be a trustworthy person or organization and the victim is urged to take actions they really shouldn't.

This type of attack is one of the most dangerous.

Due to the increasing popularity of text messaging, studies have found that people are more inclined to trust and respond to text messages of this type. According to Gartner in 2016, a whopping 98% of text messages are read, with 45% being responded to.

This brings a whole new meaning to the phrase: “Read between the lines.”

Tax Scams

Perhaps not surprisingly, tax season means high season for tax scams. As with other scams discussed on this page, being cautious when unsure is the recommended course of action. There is no shame in being scammed, because those who enact scams are, unfortunately, extremely sophisticated.

Learning their methods and what you can do to protect yourself is important. Also, reporting suspected scams supports and helps protect everybody. You can read more about that in the final section.

According to the IRS itself, tax scams come in many forms, including:

- Fake text messages.
- Social media accounts.
- Emails.
- Phone calls.

In the face of so many everyday ways to enact a scam, you should protect yourself. Below, we’ll quote directly from the IRS, so you can be certain that **the IRS DOES NOT**:

- Initiate unexpected contact with taxpayers by email, text messages or social media channels to request personal or financial information.
- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. The IRS does not use these methods for tax payments.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving the taxpayer the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.
- Leave pre-recorded, urgent or threatening phone messages.
    - In many variations of the phone scam, victims are told if they do not call back, a warrant will be issued for their arrest. Other verbal threats include law-enforcement agency intervention, deportation or revocation of licenses.
    - Criminals can fake or "spoof" caller ID numbers to appear to be anywhere in the country, including from an IRS office, which makes it difficult for taxpayers to verify the actual caller's number.
    - Fraudsters have spoofed local sheriff's offices, state departments of motor vehicles, federal agencies and others to convince taxpayers the call is legitimate.
    - Any taxpayer receiving a scam phone call should hang up immediately and not give out any information.

Businesses of all types and sizes, especially small businesses, need to be aware cybercriminals could target their businesses with scams to steal passwords, divert funds or steal employee information.

The IRS has confirmed that it continues to see instances where small businesses, including tax professionals, face a variety of identity-theft related schemes that try to obtain information to file a business tax return or use customer data for identity theft.

Businesses, including tax professionals, are encouraged to follow best practices from the Federal Trade Commission, including to:

- Use multi-factor authentication.
- Set security software to update automatically.
- Back up important files.
- Require strong passwords for all devices.
- Encrypt devices.

Personal & Organizational Information Safety

Here we'll provide some additional tips on what you can do to protect your personal information and your organization's information, too:

- Read our "What We Won't Do" section again and be suspicious of anything unsolicited.
- Verify the suspicious correspondence using your own trusted sources.
- Provide information about your organization only if doing so is approved and verified.
- Ensure you are 100% confident before following links or downloading items.
- Reveal personal or financial information about yourself only in secure circumstances.
- Respond to feeling pressured by emails, calls, or texts asking for your info by reporting them.
- Send sensitive info over the web only after confirming authenticity *and* security.
- Reach out to relevant sources to confirm suspicious correspondence—never be too busy.
- Install quality firewalls, anti-virus software, and email filters, then maintain them.
- Check your email client and web browser for anti-phishing features they offer.

Mobile: On-the-Go & Good-to-Go

Staying secure while enjoying the freedom of online banking may seem like a contradiction to some. With freedom comes risk, right? No. The right steps can take you anywhere safely, so we've compiled our list of online banking security measures, which thankfully come in simple steps:

Add a Password to Your Phone

To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN). To set a PIN or password, go to your device settings. It is a good practice to change your password every 90 days.

Keep Your Mobile Device Up-to-Date

Your phone's operating system software should be kept up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

Log Out

When you are finished at a website you are logged in to, log out instead of just closing the page. As an added security precaution, NYMCU Mobile Banking will time out after 20 minutes of inactivity.

Understand App Permissions before Accepting Them

You should be cautious about granting applications access to personal information on your phone or otherwise letting an application have access to perform functions on your phone.

Report a Stolen Smartphone

The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider.

Avoid Hot Spots

Accessing WI-FI networks that are open to the public can make your phone an easy target of cybercriminals. You should limit your use of public hotspots at locations like coffee shops or airports. Instead, use protected WI-FI from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be cautious if you are asked to enter account or login information.

Enroll in Touch ID or FingerPrint Login

Touch ID and FingerPrint Login allow users to login with the touch of their finger.

Download Applications from Reputable Sources

Ensure an app is legitimate before downloading it. You can check the legitimacy of an app by checking reviews, confirming the legitimacy of the app store, and comparing the app store's official website with the app store link. Apps from untrusted sources may contain malware that, once installed, can steal information, install viruses and cause harm to your phone's contents.

Reset before You Resell or Recycle

Your smartphone contains personal data you want to keep private when you dispose of your old phone. To protect your privacy, completely erase data off your phone and reset the phone to its initial factory settings.

Reporting Suspected Scams

If you open an email you think is suspicious, don't worry. Opening your emails doesn't constitute a threat. However, **clicking a link** or **downloading an attachment** does. **Never respond** to suspicious emails or forward them to colleagues or friends.

If you receive a suspected **phishing email**, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.

If you receive a suspected **phishing text message**, forward it to SPAM (7726).

Report the phishing attempt to the FTC at ReportFraud.ftc.gov.

In **Google**, click the three dots next to your Reply option and select "Report Phishing". A panel will open, asking you to confirm that you wish to report the email. Click "Report Phishing Message" and the email will be reviewed.

In the **Outlook Web App**, click the three dots next to the Reply option and choose "Mark as Phishing". A panel will open, asking you to confirm that you wish to report the email. Click "Report" and the email will be reviewed. (The Outlook client does not offer this option.)

Apple asks that you forward the suspicious email to reportphishing@apple.com.

Report tax-related SMS/text/calls phishing attempts to phishing@irs.gov – with the subject line: IRS Phone Scam. For calls, give the caller ID/or callback number. In other cases, copy the entire message and send it as an attachment.

Contact the Treasury Inspector General for Tax administration to report the call at: IRS Impersonation Scam Reporting

You can also reach out to the MCU Contact Center with any queries about your MCU account at: 1-844-628-6969.