Protect Yourself from Phone and Internet Fraud

Unfortunately, fraud is big business. Midco is serious about protecting you from fraud, and that's why our team of experts actively monitors our network 24/7/365 for potential fraud. While Midco takes steps to prevent fraud, you are responsible to protect yourself. We hope you will use these resources and others to educate and protect yourself from unwanted calls, online scams and fraudulent charges.

Home Phone Fraud Prevention Tips

Caller ID Spoofing

Caller ID spoofing occurs when someone sends false or misleading information to your caller ID in a way that hides the fraudulent caller's true identity and/or the call's origination point. Often the caller may describe an urgent matter, such as an account cancellation, in order to persuade you to disclose personal or business information.

What action can you take? Do not provide this information in response to an incoming call you cannot identify. Instead, find the phone number of the company that is supposedly calling you, and call them yourself.

One-Ring Callback

A one-ring callback scam often begins when your caller ID displays what appears to be a missed local call. You return the call to see who was reaching you, but are greeted with a message such as, "Hello, you have reached the operation. Please hold." The fraudsters are trying to keep you on the line as long as possible on what's often an international call, usually from a high cost area such as the Caribbean. The longer you stay on the line, the more revenue fraudsters generate through what is known as International Revenue Share Fraud.

What action can you take? If you call back a missed call and are placed on hold in such a manner, hang up immediately.

Internet Fraud Prevention Tips

Internet fraud can occur at any time, but there are sensible, simple ways to protect your online identity.

Emails and Websites

Cybercriminals attempt to steal money by installing malicious software (also known as malware) on your computer or by stealing personal information from your computer.

How does it happen? Fraudsters may use social engineering to convince you to install the malware or hand over your personal information under false pretenses. You might receive an email or be asked to download something from a website.

What action can you take? Be watchful and aware. Cybercriminals often try to pretend that they're a legitimate brand or company by using graphics in an email or website in an attempt to fool you.

- Be suspicious of any request for money, financial information or other personal information – especially "urgent" requests related to a situation that doesn't make sense to you. For example, if an email asks you to confirm your order number or credit card information when you have not ordered anything recently, do not provide this information.
- Do not provide your credit card number, PIN or other sensitive information to others in an email, over social media or any other unencrypted or unsecure channel.
- When in doubt, do not provide any information without first verifying the legitimacy of the request by contacting the organization directly. Don't use contact information provided online, by a caller or included in an email.
- Always lookup email addresses or phone numbers through legitimate channels. For example, go to the company's website directly and look for contact information.
- Email can be especially misleading. The "from" and "to" addresses in an email can be easily faked and appear to be legitimate or associated with someone you may know. Links inside an email to a company website can point to fake, realistic-looking copies of the genuine website.
- Never reply to the email "sender" and never click links inside an email. Instead compose a new email using a verified email account or manually open a new browser tab, search for the organization site and go there directly.

- Be wary of emails that threaten to close your account or some other action if you fail to respond. Instead of falling for a fake alert, contact the company or brand you do business with directly – by opening a browser window and typing the website address of the company yourself, rather than clicking on a link. Verify with the company whether the information sent to you is legitimate.

Midco and other companies often log and track these reports to put additional protections or notifications in place if they're seeing trends in malicious behavior.

Passwords

- Periodically change passwords for your various online and email accounts.
- Never create passwords that contain real words. Instead use passwords that include multiple letters, numbers, capitalization and symbols (if allowed).
- Never share your password with anyone.
- Do not use the same password for your social media accounts for email accounts, other website logins – especially passwords for your sensitive banking, finance or health website accounts.

In general, if a request for information is unusual, unexpected, doesn't make sense, or sounds too good to be true, we encourage you to slow down, think, and listen to any instincts telling you to be careful.

Additional Resources

There are many other ways fraudsters can attempt to scam your business. For more tips on protecting yourself from Internet fraud, visit the Federal Communications Commission's Consumer Protection Library.

Midco's Information Gathering Policies

It's important to remember that when you sign up for Midco services, we collect the necessary information about you at that time. We don't call or email you to ask for personal information. If we ever need to update your account, we send a letter to the address on your account and ask you to contact us. Additionally, Midco handles all of your monthly billing internally. Don't fall victim to callers saying they are taking over Midco's billing and need your verification to make changes.