

How to Identify Phishing and/or Fraudulent Emails

From time to time, you might receive emails that look like they come from Cameron Communications, but they are typically falsified emails with the intent of garnering your personal information. Often, these emails direct you to a website that looks similar to an official Cameron Communications website, where you may or may not be asked to provide account information (like your email and password information). Unfortunately, providing this information to false websites may open the door for harm to come to your personal account, and it could potentially be used fraudulently. Some of these messages could also contain potential viruses or malware that can detect sensitive materials that you store on your computer, such as passwords and credit card numbers.

It is always recommended to keep an active and up-to-date anti-virus program running on your computer. If you are interested in one supplied by Cameron Communications, please [contact us](#).

If you receive an email that looks like it may have come from Cameron Communications, look for these clues that often indicate a phishing or fraudulent email.

1. Know what Cameron Communications will **NEVER** ask you over email:

- We will **NEVER** ask you for your social security number or tax identification number
- We will **NEVER** ask you for your credit card number, PIN number, or credit card security code number
- We will **NEVER** ask you for your mother's maiden name
- We will **NEVER** ask you for your Cameron Communications password
- We will **NEVER** ask you to verify or confirm your Cameron Communications account information by clicking on a link from an email.

2. Attachments on suspicious emails.

It is always a good idea to use caution when opening an email attachment from suspicious or unknown sources. Best practice is to not open the attachment. Email attachments can contain viruses that may infect your computer when the attachment is opened or accessed. If you receive a suspicious email that has an attachment and appears to have been sent from Cameron Communications, delete it immediately!

3. Grammatical or typographical errors

Be on the lookout for poor grammar or typos! Some phishing emails are translated from other languages, so you may notice that the text of the email may not make complete sense. Also look for usage of symbols throughout the text of the email.

4. Check the return address

When you suspect an email may be spam or fraud, check the return or "from" address of the email. While a fraudulent email may look like it came from Cameron Communications, you can occasionally determine if it is authentic by checking the return address. If the "from" line of the email looks like camtel-security@hotmail.com or camtel-fraud@msn.com, or contains the name of another Internet service provider or email host, you can be sure it is a fraudulent email.

5. Check the website address

Genuine Cameron Communications websites will look like this: www.camtel.com, or <http://www.camtel.com> and finally, <http://camtel.com>. Sometimes the link included in the spoofed email looks like a genuine Cameron Communications website address, but you can see where the link will go, simply by hovering over the link with your cursor. A box will pop up with where the actual link goes, and if it doesn't look legitimate, don't click!

On a genuine Cameron Communications link, you will NEVER see website addresses like <http://security-camtel.com> or a series of numbers, like <http://123.456.789.123.camtel.com>. These are examples of the many variations that you might see. If you get an email request asking you to visit these sites, please let us know!

Alternately, sometimes the spoofed email is set up such that if you click anywhere on the text you are taken to the fraudulent website. If this happens, immediately close the browser.

6. DO NOT "UNSUBSCRIBE."

Never follow any instructions contained in a forged email that claim to provide a method for unsubscribing. Many spammers use these "unsubscribe" processes to create a list of valid, working emails.

7. Protect your account information

If you did click on any link of a spoofed or suspicious email and you entered your Cameron Communications account information, you should immediately change your Cameron Communications account password. You can do this through the online billing section of "My Account."