Consumer Email Tips

Please note: This guidance document is not intended to replace sound legal advice. Please consult your attorney for legal questions.

Overview

Email is still the most widely used digital communications channel. It's no surprise, with nearly 4 billion email users worldwide and over 280 million emails sent daily. Interestingly, research shows most consumers have two email addresses. Often they have a secondary email address, used as a "catch all" address, while the primary is retained for more personal communications. Social media requires an email address in order to engage in the Twitterverse, Facebook and other places people gather to share content and opinions on the internet. It should come as no surprise that the common denominator across ecommerce, social networks and other Internet-based activities is email.

Why am I receiving this email?

The most common question consumers ask in response to receiving a particular marketing email is, "Why did I receive this email?" The simple answer that covers most of the reasons is that at some point, you provided your email address and "opted in" to receive email messages.

You may have subscribed to an online newsletter, purchased a product at a retail store or made a recent online purchase from a retailer's website. When you signed up, you provided your email address as a point of contact. The sender may email you to provide you with new information about the company or organization, its products and services as a result. You may also have given the company permission to email you about other related products, services or other information. In addition, it's important to note in the United States, companies are allowed to send unsolicited marketing communications to recipients as long as they provide a method for consumers to unsubscribe or opt-out of receiving future emails (typically a link or email address to contact with an unsubscribe request). Then, if you do not wish to receive additional marketing emails from the company, you simply click on the unsubscribe link in the email to opt out or change your communication preferences going forward.

Practical Ways of Keeping Yourself Safe

Email can be a vital communications tool for consumers, allowing interaction with other individuals, companies and organizations. With the nearly universal use of email, what steps can consumers take to help keep themselves safe from potential fraud or other malicious communications?

1. **If you're not sure, don't open it.**
   If you don't recognize the sender of a message and it has an attachment, do not open the attachment. It's important to realize email attachments can pose a threat in your inbox. That "chain" email your uncle in Toledo forwarded to you may have actually originated from a criminal organization inside or often outside the United States. When you open the attachment (a PDF, Word doc, or some other common file type) you may also be launching hidden software on your computer that accesses personal information on your machine, starts running other malicious software in the background, or even locks you out of your files and documents until you pay a ransom to regain control. Be aware of the emails you are opening and attachments you are downloading and where they come from, and you'll go a long way toward protecting yourself from these types of malicious emails.

2. **Never reply to requests for information via email.**
   It is important to note your bank, health care provider, employer or other official entity should never ask you for your password, bank account number, Social Security number or other personally identifying piece of information over email. The more common and safe practice for a company to request this kind of information from you is to ask you to visit and sign in to a website, and then provide or update your information there. Never send passwords or credit card numbers through email. Even if the request is legitimate, it is a misguided request, as emails can be intercepted and read by a malicious third party. If someone asks you for a credit card number to complete a transaction, ask them for the correct website to visit and verify it is a secure site before you provide payment information. Consider using a safe electronic means of payment such as Paypal or Venmo, or call them and read the number to them on the phone.

3. **Are there any clues to identify a fraudulent email?**
   In the majority of phishing and other email-based attacks, the fraudster doesn't know much, if anything, about the individual people to whom they are sending emails . Using phrases such as "Dear Customer" on a fraudulent bank statement, or "Dear Sir/Madam" is a sign the email may not be legitimate. Your bank uses your first and last name to help establish trust and identify themselves as the legitimate institution you bank with. Familiarity breeds trust in this case. Read the full text of the email, not just request for information. Often times these messages are crafted overseas and the spelling, grammar, and wording is obviously poor, as the text may have been put through a translator or written by someone who does not have a firm grasp of the English

language. It is safe to assume your bank will follow professional standards and the messages from it should be coherent and professional.

4. **If it sounds too good to be true, it probably is.**
   This is good advice for life in general and particularly applies to email marketing. If you receive a strange email offering you some incredible opportunity to make a large sum of money with no risk and no effort, you should be very suspicious. One common form of this email scam that has been going on for decades involves receiving an email from a supposed prince, king, or other royalty from another country who needs your help to access a large sum of money they have in some bank. They will pay you a massive amount of money to help them access the account. All you need to do is provide them a small sum of money in order to help get the process moving. Far too many people have fallen prey to scams like this, providing initially small and later large amounts of money to these criminals in the belief they will receive a windfall that never comes.

Email Terms for Consumers to Know

- **Phishing**
  - The practice of sending fraudulent emails purporting to be from reputable companies in order to induce individuals to reveal personal information such as passwords and credit card numbers.
- **Spam**
  - The popular name for unsolicited commercial email. However, the definition of spam has evolved over the years to include any mail that is unwanted versus wanted.
- **Unsubscribe (Opt-Out)**
  - The act of requesting to be removed from a marketer’s email program or newsletter. Facilitated by clicking the unsubscribe link or requesting manually to be removed by the sender. Quick tip: Companies have 10 business days to process and honor an unsubscribe request. So, when you unsubscribe from a company’s email program today, you may still receive emails for the next 10 days. Also, simply opting out of receiving marketing emails from a company does not preclude the company from sending transactional emails (order confirmation, invoice, customer support information, etc.).
- **Opt-In**
  - A cornerstone of permission-based email marketing, opt-in is the term used when an individual provides explicit consent to join an email marketing program. An example would be when you submit your email address and check a box confirming you would like to receive a newsletter or other email content from a company.
- **Sender Name**

    - The portion of the email address displayed in most, though not all, email system "inboxes" in place of, or in addition to, the sender's email address. Friendly "froms" can be customized and changed, whereas the sender's actual from address and domain typically do not. An example: "ANA," also referred to as "display name."
- **Subject Line**
    - An introductory sentence used to describe the contents of the email message. This information is often shown in email system inboxes, along with the sender or "from" name.
- **CAN-SPAM**
    - Popular acronym name for the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, U.S. legislation regulating commercial email. Imposes a number of detailed requirements on persons and entities that initiate and send commercial email messages. Violations can result in fines.

Additional Resources

The ANA Accountability staff and its Email Experience Council would like to hear from you if you are receiving unwanted emails and you cannot opt-out. To file a complaint, you can email a description of the matter and a sample of the unwanted email to ethics@thedma.org.

If you are receiving unwanted/spam emails and wish to file a complaint to the Federal Trade Commission (FTC), please go here:
https://www.ftccomplaintassistant.gov/GettingStarted?NextQID=57&Url=%23%26panel1-5#crnt

If you believe you are a victim of identity theft or you've been hacked, you can contact FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/complaint/ or the FTC at: https://www.identitytheft.gov/.