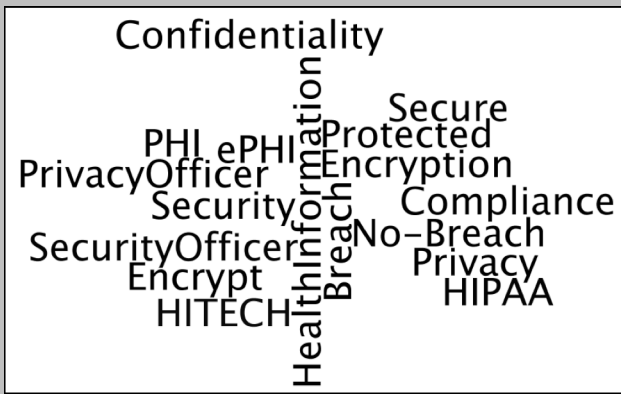


e-Mail Security Tips



#1: Prevent virus outbreaks and spam

Viruses are often spread through e-mail. You can greatly reduce the spread of e-mail viruses by using antivirus software, using only e-mail services that offer automatic antivirus protection (such as AOL, Google, Hotmail, and Yahoo), opening e-mail only from trusted sources, opening only attachments you're expecting, and scanning attached files with antivirus software before opening them.

Spam is loosely defined as unsolicited bulk e-mail and loosely correlates to the junk mail that turns up in your home mailbox. But spam represents more than unwanted clutter. It clogs e-mail accounts—and networks and servers—while trying to sell products, spread jokes, or propagate Internet hoaxes.

Reduce the amount of spam you receive by being cautious where you post your e-mail address. Avoid publishing your e-mail address on Web sites or submitting it to every site or organization that requests it.

Never forward chain messages, which often reveal coworkers' and colleagues' e-mail addresses to other parties. Use caution when accepting e-mail offers or agreeing to accept mailings from vendors; subscribe only to Web sites and newsletters you really need and consider creating a generic Hotmail or Yahoo e-mail account for these subscriptions.

Don't open unsolicited e-mail. If you accidentally open spam, don't click links offering to unsubscribe or remove you from the mailing list unless the sender is a trusted vendor.

#2: Avoid phishing attacks

Phishing scams are designed to steal consumers' personal information. They often use doctored and fraudulent e-mail messages to trick recipients into divulging private information, such as credit card numbers, account usernames, passwords, and even social security numbers.

Online banking and e-commerce are generally safe, but you should always be careful about divulging personal

and corporate information over the Internet. Phishing messages often boast real logos and appear to have come from the actual organization, but those messages are frequently nothing more than copyright infringements and faked addresses. If you suspect a message possesses any credibility, you are much safer calling the company directly—preferably at a telephone number printed on a paper statement or invoice—and talking to an authorized representative.

#3: Manage your Inbox

Sort messages by priority, subject, date, sender, and other options to help find important e-mail that requires your attention. Proper e-mail etiquette dictates that you respond to all e-mail in a timely fashion. Generally speaking, you should respond to all professional e-mail within a business day, even if it's just to say you've received the message and will look into the matter. Occasionally, you may receive an e-mail thread that contains responses from several people; always read the entire thread before responding.

#4: Compose professional messages

It's easy to convey the impression that you're unprofessional or careless if you don't follow some basic principles of good business writing. Make sure you follow proper grammar and sentence structure when composing and responding to messages and use a spell checker. Don't type in all capital letters—it creates the effect of shouting. Break your message into paragraphs for logic and readability.

Before clicking the Send button, give it a final once-over. Reread the entire e-mail, checking it for grammatical errors, punctuation mistakes, and typos. You'll be amazed at what you catch. Also make sure your tone is appropriate for the message.

#5: Write effective subject lines

Writing subject lines can be tricky, but you should always include one. The goal is to summarize the message without being too wordy or too vague. Long subjects tend to be skimmed or ignored, and they don't always fully display in e-mail viewers. For best readability, use sentence case for subject lines rather than all caps:

Not

AGENDA FOR MEETING ON 3/29/07

#6: Properly use CC and BCC

The carbon copy (CC) and blind carbon copy (BCC) features found in most e-mail clients allow you to send copies of an e-mail to others you need to keep informed but who aren't necessarily the primary recipients.

When copying others, be certain the e-mail message pertains to them. If you use e-mail address lists, verify that all of the members of the list should receive the e-mail, too, and remove those who don't need to be included. And use the BCC feature sparingly. If sensitive topics require BCCing others, it may be best to take the matter offline and discuss it in person.

#7: Obey etiquette rules when forwarding messages

Before you forward an e-mail, make sure that all recipients need to receive the message. In addition, be careful when forwarding sensitive or confidential information. Never forward proprietary information to external audiences or to unauthorized recipients. Before clicking the Send button, review whether a message's contents are appropriate for each listed recipient.

#8: Don't be a party to a flame war

Flame wars are heated e-mail exchanges that are more emotional than reasoned, and they have no place in professional communications. If you receive a flame or suddenly find yourself in a flame war, take a little time before responding, if you respond at all. Think about the situation and reply rationally not emotionally.

You may also decide not to reply but to deal with the issue in person. Often, flame wars are started because of a simple misunderstanding. An ill-phrased comment (or even a well-phrased one) can be misconstrued by a recipient, who then fires off a salvo in response. Instead of replying, go talk to the person and discuss the message. If talking with the person doesn't end the problem, involve a manager for assistance in resolving the issue offline.

#9: Protect e-mail addresses

Don't divulge your coworkers' e-mail addresses to vendors, friends, or others outside the organization. Verify that recipients listed in the To and CC fields should be receiving messages and that you won't be revealing others' e-mail addresses in the process. Don't post your or coworkers' e-mail addresses on Internet forums or bulletin boards, on Usenet groups, in chat rooms, or in other public areas.

Here are a couple of simple ways to help keep others' e-mail addresses private. First, use the BCC feature when you need to hide their e-mail addresses from external audiences. Second, delete their addresses from

messages you forward. It takes only a few moments and will reduce the chances of coworkers' e-mail addresses proliferating in the wild.

#10: Be smart about handling attachments

E-mail attachments consume inordinate amounts of e-mail server space and network bandwidth and are often the culprits behind virus outbreaks—but they're often the easiest way to transfer files. Just be sure to follow these guidelines when e-mailing attachments:

- ✓ Don't attach large files to an e-mail; anything over one or two megabytes shouldn't be sent via e-mail.
- ✓ Limit the number of files you attach to a message to five or fewer.
- ✓ Save attachments to your hard drive and then delete the e-mail message containing the attachment.
- ✓ Don't open unexpected attachments or those sent by unknown parties.
- ✓ Always scan files with an antivirus program before opening an attachment. Never click an attachment without first confirming that it's virus-free.
- ✓ Don't annoy recipients by forwarding attachments they can't access. If an attachment requires a new or less-common application, say so in your message.

#11: Don't include sensitive or potentially embarrassing information

Don't make the mistake of thinking your e-mails are private. They're not. Think of them as postcards. You should never include any information in an e-mail that you wouldn't want published on the front page of your local newspaper. In other words, never send confidential, proprietary, sensitive, personal, or classified information through e-mail. You should also refrain from making inflammatory, emotionally charged comments in e-mail.

#12: Know when to use e-mail (and when not to)

Businesses provide e-mail for professional, business-related use, not for jokes, gossip, or chain e-mails. Also remember that you shouldn't send an e-mail to do a conversation's work. Complicated subjects are often difficult to explain face to face, much less in an e-mail. Instead of firing off a complicated explanation via e-mail, set up a short meeting to address the issue in person.

E-mail is also a poor stand-in for conversation when conducting critical, difficult, and/or unpleasant discussions, such as issues related to human resources matters. Touchy communications are best handled in person.

Special thank you to TechRepublic for sharing these 10+ e-mail best practices to share with your users, accessed at <http://www.techrepublic.com/article/10-plus-e-mail-best-practices-to-share-with-your-users/> on 01/13/2015.