

Privacy in the Modern Age, Part 4

Edward D. Duvall
24 Mar 2021

4 E-Mail

There are only two kinds of emails: professional and personal.

If you have a professional email account at your workplace, then everything stated in that email should be professional in tone, all business. Your boss and others in your company have access to all of them, and if you put personal items into a workplace email or attach offensive pictures, then that is a problem you have created and should correct immediately. Keep the workplace emails professional. No one is going to get too concerned about occasional innocuous jokes about how computers don't work, or why the soda machine eats your quarters. But never mention any personal comments about other workers, or the boss, or company policy, unless your boss specifically directs you to do so. Never put the company's trade secrets in an email, unless directed by the company's owner. But if you are directed to put trade secrets in an email by some generic manager, make some excuse not to, and remind him that trade secrets are to be protected.

I have an email that I use for professional purposes. Since I am an independent writer, I put things in my emails that are intended for public viewing, and I don't much care what people think about them. They are written specifically for public consumption. But the normal workplace is very different: keep to the relevant subjects at hand that pertain to your work, and leave it at that.

Personal emails are a different thing altogether. You will note that "hotmail", "gmail", and many others are given "free", meaning that the provider pays the near-term direct costs, while you pay the long-term indirect costs. When you delete an email from your "free" account, it may appear to be gone, but in fact all emails are retained permanently. A clever enough hacker can obtain all your emails, current and deleted; and of course, the provider has access to them always. Once again, we do not really know who has access to them or if the providers have agreements with marketing corporations or government agencies to provide copies of all emails for review. The FBI has been using in-house software since the 1980's (called OMNIVORE and CARNIVORE) to intercept emails and all internet traffic from a particular ISP. It has now been replaced by a commercial code NARUSINSIGHT. Supposedly, the software is designed to intercept only traffic between a certain individual against whom the FBI has secured a search warrant. But in this age of mass electronic intercept and storage capabilities, it is reasonable to assume that all emails are searched for certain keywords that some government agency deems "offensive" or "threatening". Remember: if a technology exists, it is first used against recognized national enemies, but the second use is against all citizens. There is no way to know who has access to your emails, or for what purpose. At minimum, your emails are probably being scanned by corporations for the purpose of directing advertisements in your direction. That is annoying but harmless; however it is common now for people to have their careers ruined for something they put in an email twenty years ago; and our current ruling elite seems fascinated and overjoyed at the power of intimidation and cancellation they now wield without consequence.

So what is the best you can do to preserve your privacy regarding personal emails? Here are some simple rules:

- a. Use end-to-end encryption if possible. But don't rely entirely on encryption: someone somewhere has the means to either break the code or obtain the keys.
- b. Never put anything in an email of any importance, such as full name, address, phone number, date and place of birth, Social Security Number, mother's maiden name, names of relatives, places you have pre-

viously lived, banking information, or schools you attended. If this information is to be provided for some legitimate purpose (such as applying for a loan), make sure it is provided only on a secure website, not by email. Even better, send it by U. S. first-class mail.

c. Never attach pictures of yourself, your relatives or friends, or any that show your home, car, or street. If you want to send pictures, have them printed and send them by U. S. first-class mail.