Dos and Don’ts for Protecting Your Personal E-Mail Account

According to a 2014 study, each of us sends and receives about 200 e-mails per day! Think about it. Not only do we write back and forth to friends and acquaintances via e-mail, but we also transact personal business with banks, credit card companies, charities, and more. And this means that we transmit and store a host of personally identifiable information—our full names, birthdays, account numbers, receipts, medical correspondence—in our e-mail accounts.

If a clever hacker were to gain access to your e-mail account, how much of your personal confidential information would be vulnerable? To help protect your information from the many cyber threats around today, here are some important dos and don’ts.

Do:

1. **Wait until you’re on a private, secure network** to access, send, or read e-mail messages that contain sensitive information.
2. **Audit your messages.**
    a. Retain as little information about yourself as possible in your account so that a potential hacker couldn’t obtain enough personal data to con you (or those you know) or to steal your identity.
    b. Regularly clean out your messages from your inbox. This is particularly important if you have opted for paperless billing and statements from your financial institutions. **A best practice is to delete the pertinent e-mails once you take care of any online financial business.**
    c. Regularly delete items in your Trash and Sent folders as well.
3. **Use a strong password**, which makes it much more difficult for intruders to access your account.
    a. A strong password has at least **8** characters; contains a mixture of numbers, upper- and lowercase letters, and special characters; does not contain words in any language, slang, dialect, or jargon; and is not based on anything personal, such as your pet’s name or hometown.

Don't:

1. **Check your e-mail on a public Wi-Fi network.** Hackers have ways to sniff your activity more easily on public networks so that they can read your e-mails, dig around in your account, and even see what you enter for your password when you log in.
2. **Use the same password for different accounts.** When you open an online account with a company, the company will likely use your e-mail address as your username for the account. Because so many organizations follow this practice, if a cyber criminal were to obtain your personal e-mail address, he or she could be a giant step closer to accessing your "world." He or she might then attempt to crack your password and break into your various online accounts. Play it safe and create a different password for each online account you open!

Use multifactor authentication

Although a strong password is your first line of defense against hackers, a username with a strong password may not be enough to ward off criminals whose tools and tactics are becoming more sophisticated by the day. That's where multifactor authentication can come into play. It adds another layer of verification. When you log in, after entering your username and password, a code will be sent to your smartphone, which you need to provide before you can access your account. So even if your username and password are compromised, unless a hacker has your phone, he or she wouldn't readily be able to get into your e-mail account!

Questions?

If you have any questions about the information shared here, please feel free to call me at 610-280-9330.

Sincerely,

Steven M. Seide, CFP®, AIF®