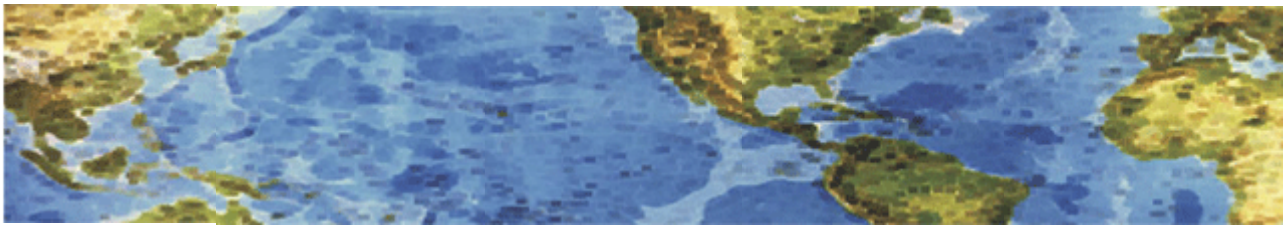
HALL ASSOCIATES



Risk-Based Decision Making Commentary
17 July 2013 Newsletter

11 Really Dumb Things Not To Do With Your E-mail

http://www.foxbusiness.com/personal-finance/2013/07/03/11-really-dumb-things-do-with-your-email/?intcmp=obinsite

Our simplest and most common vulnerability to criminals, hackers, spammers and spying eyes is e-mail. Just in the past few months, databases at LivingSocial and Evernote were hacked, exposing roughly 100 million e-mail addresses to identity thieves. Facebook allegedly exposed 6 million users' e-mails to unauthorized users, a "glitch" the company admitted was not detected for a year. All this comes on the heels of mega-breaches like the one at Epsilon, which provides marketing services for more than 2,500 financial and lifestyle companies. Epsilon admitted hackers stole "only" 2% of its customer data. But since its databases may contain upwards of 250 million email addresses, that means "only" 5 million people were placed at risk.

So what's the big deal? E-mail is no longer a convenient secondary conduit for saying hello to friends. It's plugged directly into our lives. Messages sitting in our e-mail accounts can expose not just our address and contact numbers, but also our bank and brokerage account numbers, credit card information, online financial transaction receipts and confirmation of forgotten or changed passwords in all of our other accounts. ***That's why e-mail is now the single most common vector of attack for fraud***, according to the Federal Trade Commission. It's laden with valuable data. And everyone knows their chances of getting caught are slim to none.

Bottom line: The best way to stay safe is to aggressively protect yourself. No one else can guard your e-mail better than you. Here are the top 11 things you can do right now to reduce your risk of getting your e-mail either hacked or scammed.

1. Never check your e-mail on an unsafe network. - A computer in an Internet café, library or any other business may be loaded with malware to steal your passwords. Public WiFi systems are vulnerable too, even at places like coffee shops, airports, hotels and conference centers that require passwords, since any ID thief can afford a $3 cup of coffee and get the same password.

What to do: Unless the computer and network you're using belongs to you or your employer, don't sign into e-mail.

HALL ASSOCIATES

2. Don't stay signed in. - Signing into e-mail every time you pick up your phone can be a real pain. Deal with it. By staying constantly signed in, a hacker can gain immediate access to the most important information of your life.
What to do: Signing out is inconvenient. Do it anyway.

3. Don't repeat use your e-mail login name and password - Just this year, hackers cracked databases containing the passwords of up to 50 million LivingSocial users, and another 50 million users of Evernote. If the password to your checking, credit card, social media or any other account ends in @gmail.com, @yahoo.com or any other e-mail address, those thieves possess an important piece of your identity puzzle. Since many people mistakenly use the same password or User ID for multiple accounts, identity thieves know the skeleton key that may fit many doors.
What to do: Never use your e-mail address and corresponding password for any other accounts. Beyond that, don't use passwords based on things like your birthday, your kid's name or your street. The more random, the better.

4. Not deleting old e-mails properly - Many people never delete old messages in their inbox, or delete their caches of trashed and sent e-mails (though most e-mail systems purge deleted email after 30 days). Those messages may contain addresses, account usernames and passwords, contact information for all your friends, financial data and a host of other sensitive information.
What to do: Delete sent, trashed and old messages. Delete e-mail with any sensitive information (like your tax paperwork, health insurance applications, etc.) immediately after sending it. Better yet, don't send sensitive information over e-mail. For security, the old-fashioned Postal Service letter is still the best.

5. Don't fall for a "guaranteed" loan or credit card offer - If an e-mail promises a loan or credit card worth a guaranteed amount of money at a low interest rate, it's a scam. Nobody will give you credit without first checking your credit report.
What to do: Don't click on links in these messages, and delete them.

6. Don't click on ambiguous e-mails from "friends. - Since hackers have raided our e-mail contact lists, even messages from our best friends could be vectors of attack. Hackers often pose as friends stuck penniless in Europe or Asia and in need of an immediate wire transfer, or friends imploring us to "Check out this funny video!" with links stuffed with spam or laden with malware. Sometimes the tipoff is an e-mail from a "long-lost friend," or a close buddy using a very old account. Some of these e-mails come with no text at all… just a link.
What to do: Read e-mails from enemies closely, and e-mails from friends even more closely. If you receive a suspicious e-mail from a friend, don't click on any links or download any files. Delete the e-mail, and call your friend. If it turns out the e-mail was legit, he or she can resend it.

HALL ASSOCIATES

7. "Verifying" personal information via email - It looks like your bank or credit card company asking to verify your account information. Or it could be from UPS or FedEx trying to "confirm" your address for a missed delivery. It could even be from the IRS claiming you owe them, or they owe you, money. ***None of these institutions send personalized e-mails, and none ask you to "verify" personal information by email.***
What to do: If an institution handles important things like money or packages, it doesn't use e-mail to communicate, and certainly not to confirm personal information. Delete the suspicious e-mail, and call the business or institution in question to inquire about the matter at hand.

8. **Don't e-mail strangers about money** - Many scams involve sending money to people we've never met. There's the "Wall Street insider" with the hot investment tip, the foreign company that needs you to cash a check or process transactions, the marketing company asking you to be a secret shopper or offering an irresistible work-at-home or franchising opportunity, the e-mail chain letter inviting you to "get in early" on a pyramid scheme, the Irish Lottery, even the lawyer of a deposed politician trying to get his money out of the country (this age-old ruse is actually growing more sophisticated, with better-written e-mails and virulent malware). Every one of them is a scam.
What to do: If someone you've never met offers you money, delete immediately!

9. Don't get tricked into thinking your credit card has been stolen - You may receive an e-mail that says "Thank you for your recent order!" Except — you never ordered anything. You assume your credit card has been stolen and you open the e-mail and click the button that says "Cancel Order." You just became an ID theft target.
What to do: Think twice before clicking any button, link or attachment in an e-mail. Even if it's from a business you know, or one from which you have ordered something. If you need to cancel, call the company and cancel, or do so on their website. If you're really worried that you've been victimized, you can check each of your credit reports for free once a year.

1**0. Don't donate to fake charities** - After Hurricane Sandy and the giant tornado in Oklahoma, fraudsters sent e-mails requesting donations for relief efforts. The money went instead to scammers all over the world.
What to do: Only donate to established, well-known aid groups, and do so on their website or over the phone. Don't navigate to these sites from e-mails, and don't call the phone number in the e-mail. Look those up.

11. Don't click on too-good-to-be-true deals - Many of us receive legitimate e-mails alerting us to cheap flights, hotels and cruises. But when the offers seem just unbelievably low, and they come from companies and e-mail addresses you don't know, don't get sucked into clicking.
What to do: What's that old line about something seeming too good to be true? If some new travel site is running a special deal, rather than click a link in an e-mail, search for the deal on the Web. Find out if anyone has reported it as a scam. Make sure it checks out before you click.

There's no silver bullet here even if you do all of these things. It is impossible to completely protect yourself on the Internet. Remember, you are connected to the World, not just your friends. That said, the better you can minimize your exposure and operate cautiously, the longer you can stay safer.