Anand Wadadekar

Internet Safety

> "Internet security has become a serious issue for anyone connected to the net. Even if you don't think you have anything worth protecting on your computer, it's still important that you keep it locked down!!!."

Communication today plays a very vital role and more so, communication done through electronic media like internet, cell phones, etc.

As the famous quote goes, "A word uttered cannot be taken back", this has now become very much critical in the electronic / internet age. This article speaks about internet security and so would like to construct another quote, which is, "Information given cannot be taken back".

We hear almost daily that someone lost money or was cheated due to misuse of personal information on internet or hacking in the email account or stealing credit cards, etc. These unfortunate events can be easily and certainly avoided if we follow simple rules of internet, while transacting or interacting through electronic media.

We will see some of the most recommended safety tips:

Computer Safety:

ANTI-VIRUS SOFTWARE-Anti-virus software should be installed on all Internet connected computers. Because new viruses are emerging daily, it is essential to configure your anti-virus software to both check for and update your anti-virus signatures daily.

ANTI-SPYWARE SOFTWARE -The term "spyware" covers a broad category of malicious software designed to intercept or take partial control of a computer's operating system without the informed consent of that machine's owner or legitimate user. All home computers connected to the internet should have a reliable program to scan for the presence of spyware on their computers.

FIREWALLS -A firewall is a protective layer between your computer and the rest of the Internet. There are a number of subscription based products that are offered (McAfee, Norton, Microsoft firewall available with Windows XP Service Pack 2, etc.) At a minimum, you should have a software firewall installed on your

About Author

Anand Wadadekar is MA (Economics), MBA (Finance), AMFI

home computer to prevent an outside intruder from gaining access.

REMEMBER ME:

Unclick or don't click the tick box which asks you to save your login and password. This should be avoided on public computers.

We hear almost daily that someone lost money or was cheated due to misuse of personal information on internet or hacking in the email account or stealing credit cards, etc. These unfortunate events can be easily and certainly avoided if we follow simple rules of internet, while transacting or interacting through electronic media.

Online Communications: Email, SMS, Chatting

- Remember never to give out personal information such as your name, home address, school name, or telephone number in a chat room or on bulletin boards. Also, never send a picture of yourself to someone you chat with, unless you know the person or trust the person.
- Do not meet someone or have them visit you without the permission of your parents.
- Remember that people online may not be who they say they are. Someone who says that "she" is a "12-year-old girl" could really be an older man.
- Remember to sign out / logout when you have finished using the email service or any websites in which you have logged in.
- REPORT SPAM If you feel that a particular email is from an unidentified person or a weird email address, make sure you report it as 'Spam' in your email.

Banking:

PASSWORDS -Your password is the key that allows access to your financial information. Don't use a password that is easy for others to guess e.g. birth dates, social security numbers, mother's maiden name, child or pet names. Instead, use a password that contains a variety of letters, numbers and symbols and change it regularly. Do not tape it to your computer monitor and do not file it in your rolodex under "Password."

ENCRYPTION- If you access your financial accounts through a secure web page with your bank, the information you transmit is almost certainly encrypted. However, email is frequently unencrypted, so even if you access it from a secured web page, be wary of sending sensitive information such as account numbers, passwords and other personal information through email.

DISCONNECT- Always log off properly after you have completed your online business. Follow the secure area exit instructions to ensure the protection of your financial information.

SPAM WITH VIRUSES- Before opening emails or attachments make sure they are free of any viruses or known exploits. The best way to do this is to make sure your anti-virus software is current and scans your email as it is received.

PHISHING- Fraudsters will design fake websites that use a web address deceptively close to that of a genuine business. Their goal is to lure you into giving them personal information, such as your account number and password. The crooks can then put charges on your credit card, steal from your accounts and even steal your identity. Always ensure that you are really on your bank's website before logging on. When in doubt call your bank.

SHARING OF LOGIN INFORMATION Banks won't ever ask for your login details or your bank account details on email. If you receive such emails, do not reply to them.

Online Shopping:

- Where possible, use a secure online payment service like Visa, Verisign, PayPal, etc.
- Use credit cards rather than debit cards.
- Don't keep your personal or financial information (including account passwords) on your computer. Use removable storage (like a USB stick).
- Don't give out personal or financial information to vendors over the phone, through the mail, or online unless you are absolutely certain that your contact is legitimate.
- Try to make all of your online transactions with one credit card, if you have more than one.
- Keep a record of what you pay for and always check your online purchases off against your statement[s].
- Always check the privacy policy of any Web site that requests personal details. If the Web site is requesting this type of information and does not have a privacy policy, it is not wise to submit your information.
- When submitting information online, make sure there is a "lock" icon on the browser's status bar (and that it is "locked").
- Ensure that while making payment the website name starts with “https” and not “http”… see whether there is a 's' after 'http'.
- Don't give your account number over the phone unless you've initiated the call. If you've dialed a wrong number, don't give it out at all.