Are You Virtually Handicapped?

A 21st century entity (individual or organisation) is supposed to be a tech-savvy, smart and highly mobile creature. Such a highly-connected entity creates a virtual personality of itself in the digital world. But without proper knowledge about the working of the virtual world and its consequences, most of the current virtual citizens are actually 'sitting ducks'. It would not be inappropriate to call most of these professionals, organisations and individuals as 'virtually handicapped'. This article talks about the kind of risks faced by individuals, professionals and organisations alike in the modern virtual world. The current state of awareness among the young and the old, in India and all over the world, indicate a kind of helplessness in the face of virtual threats. This feeling prevails among the most powerful down to the powerless citizenry. This article thus attempts to suggest some remedies against such state of being 'virtually handicapped'. It further highlights the emerging risks from upcoming technologies like cloud computing among others.

The Context

What is meant by being 'virtually handicapped'? Virtually handicapped simply means the state of 'virtual paralysis of a 21st century netizen, *i.e.*, citizens of the Internet, (organisation, professional or individual) in the face of any electronic threat to its virtual existence'.

Most of us today use some or the other form of electronic digital systems in our daily life. Organisations, corporate or otherwise, are even more electronics-dependent. However, only a small fraction of the current users understand or have the necessary skills to overcome any virtual threat. In fact, most of the 21st century entities are unaware of the risks they face while using electronic systems.

The objective of this article is to present a compilation of the current and potential virtual dangers facing any 21st century entity. It further attempts to suggest ways of prevention and possible remedial measures to rescue oneself from being permanently virtually handicapped.

The article has been structured in five sections. The first part outlines the context. The second part provides some survey findings highlighting the state of virtual paralysis we are currently in. The third section provides a compendium of selected cases, both from domestic and international sources. The next section provides possible remedial measures that can be undertaken by individuals and organisations to prevent and/or to recover themselves from such paralysis. The fifth part details some of the upcoming technologies posing virtual danger to the entities. The concluding section summarises the contents of the earlier sections.

Dr. Debashis Kundu

(The author is faculty in Department of Commerce, Vivekananda College, Kolkata. He can be reached at debkundu_2000@yahoo.com)

Current Scenario

It is said that most of us 'shut the door after the horse has bolted'. Let this not be the case of our virtual presence too. Because while in the physical world there may be some chance of recovery of stolen goods, in the virtual world your assets and sometimes even physical items transacted through the digital route, may get lost forever. Worse still, you may be facing the legal music for a crime committed by somebody else through the digital by-lanes.

The next two sub-sections present some domestic and international cases of such virtual paralysis.

(a) Domestic Scenario:

This section is based on the contents of a survey conducted by IMRB and commissioned by VeriSign, an Internet infrastructure service provider, on over 5,000 professionals and individuals across ten Indian cities of Delhi, Mumbai, Chennai, Bangalore, Hyderabad, Pune, Ahmedabad, Lucknow, Ludhiana and Indore.

The survey clearly shows the increasing use of digital networks by Indians. About 60% of respondents accessed the Internet at least four to six times a week, mainly to shop (44%) and through user generated content (53%) such as social networks, twitter and blogs.

About 91% of the respondents said they had experienced some case of cyber fraud, such as phishing, key logging, identity-theft and account takeovers. But the most alarming situation is that a majority of respondents were unaware of ways to combat it, being virtually handicapped.

Some of the risky habits highlighted that, 38% of respondents use the same password for multiple log-ins, 83% do not look for secure websites (like, https), and only 11% check the authenticity of the website by looking at the security provider.

The silver lining to the survey was that the users may be unaware of how to protect themselves online, but their desire to be safe was high. Thus 84% of respondents wanted to use two factor authentication (2FA) *i.e.*, an additional dynamic password is generated at the log-in stage by a device, to secure their online transactions. In fact RBI has very recently made the use of 2FA compulsory for online banking.

(b) International Scenario:

The use of the digital world is even more pronounced in the Western economies. However, the state of virtual paralysis is not quite different from that of us. The RSA 2010 Global Online Consumer Security Survey covered opinions of over 4,500 adults, including professionals, from 22 countries across five continents, on the online security risks they face, their level of awareness concerning the latest threats, and what is expected from online service providers.

The respondents were found to make regular use of online banking, online shopping, social networking, governmental and healthcare portals. The survey indicated that consumers were more aware of threats. Table 1 gives details of their level of awareness regarding online threats. The respondents were allowed to choose multiple responses, thus the total exceeds 100%.

Sl. No.	Response	Frequency (in %)
1.	Phishing emails	76
2.	Phishing via SMS / text message	33
3.	Phishing over the phone (i.e., "Vishing")	25
4.	Trojans	81
5.	Keyloggers	26
6..	Malware	54
7.	Spyware	74
8.	Adware	52
9.	Botnets	14
10.	Viruses	88
11.	Worms	65
12.	Other	1%

Source: www.rsa.com

Online banking generated most concern among consumers (86%), followed by social networking activities, and governmental and other corporate activities. It was also observed that stronger online security inspires consumer confidence and thus is good for business.

Since most of the online users are young people and professionals, a survey on 'Generation Y' (18-24 year age group) conducted in the United States, the birthplace of the digital age, offered an alarming insight. Table 2 highlights the plethora of online, sometimes risky, activities conducted by them. It was conducted by TRU Research, USA.

Sl no.	Type of Online activity	Do sometimes (in %)	Do frequently (in %)
1.	Email	98	81
2.	Visit social networking sites	95	75
3.	Visit news sites	93	44
4.	Make purchases	91	26

Sl no.	Type of Online activity	Do sometimes (in %)	Do frequently (in %)
5.	Play online games	86	25
6.	Search for jobs	83	27
7.	Conduct bank transactions	82	41
8.	Enter contests or promotions	80	13
9.	Listen to music on sites	78	27
10.	Upload photos to photo-sharing or social network sites	78	21
11.	Buy or sell items at online auction sites	77	14
12.	Upload videos online	63	14
13.	Visit entertainment sites for celebrity news/gossip	60	11
14.	Use file-sharing app allowing others to access their computer/files	46	10
15.	Download/upload information to/from an "illegal" site	43	10
16.	Post blogs or video blogs online	42	7
17.	Use a micro-blogging site like Twitter	42	13
18.	Click on/respond to pop-up ads	29	2
19.	Visit private bulletin boards to share illegal or unauthorised files	25	4
20.	Download apps for "illegal" and/or "warez" sites	22	3

Source: www.rsa.com

It was found that about 95% of Generation Y spends at least one hour a day on personal online activities. A large number of young adults (73%) are concerned about being a victim of online fraud. Despite this, they (57%) are refusing to pay for services that are supposed to protect them from online fraud.

A Few Illustrations

This section highlights some of the well-known incidents of virtual dangers that organisations, professionals and individuals have faced.

The Nira Radia tape leakage controversy containing details of highly sensitive conversation by top Indian businessmen and politicians proves that no form of online conversation is actually confidential.

The security threat posed by highly-encrypted Blackberry mobile service is causing headaches to governments across the world.

The satellite failures of ISRO in the recent past have been attributed by some sources to the action of viruses sent by enemy countries online.

There have been many cases of ingenious ATM frauds committed by local highly-literate criminals.

The many cases of false prizes from online lotteries and cases of identity theft are well known by now.

Cyber-attack on key government websites in Estonia during April to May 2006 through a massive coordinated Distributed Denial of Service (DDoS) attack was one of the latest examples of cyber warfare. The attack involved an estimated one million botnet 'zombie' computers.

The latest news has been the partial shutdown of the Iranian nuclear operations by Stuxnet virus, created through an Israeli-US joint venture, and delivered online.

But the case of 'Wikileaks' takes the cake. It has so far exposed thousands of secret online and electronic mails sent from across the world, mostly to and from USA. It is further threatening to disclose additional information on banks, corporates, professionals and others.

Possible Remedies

The above sections amply highlight the many dangers of the ever-expanding digital universe. Yet, the sheer lack of understanding among the general populace is difficult to comprehend. Organisations, professionals, salaried and the unemployed – are all virtually handicapped in the face of this mounting menace.

This section thus outlines some processes and techniques that should help the online users to take care of themselves online.

(a) Individual Level:

The following section is designed to help the students, the salaried and the professionals who make use of any of the following electronic systems in their daily life. The list of 'Dos and Donts' may be a bit elongated. But just imagine what will happen when you see your years of hard-earned

money vanish into thin air just because of your ignorance. So, read on……

Tips for safe Internet surfing:

- Install and update an well-known Anti-Virus software quite often
- Use a personal firewall
- Keep your browser and operating system up-to-date with software updates
- Activate a pop-up blocker
- Scan your computer for virus, spyware, worms, etc. regularly.
- When not using the computer, shut it down or disconnect it from the Internet.

Tips for safe Internet banking

1. Avoid accessing Internet Banking account from a cyber cafe or a shared computer.
2. Passwords should be changed only from own computer.
3. After completing an online banking session, the account should be logged off. The browser should not be just closed.
4. The correct URL should be typed in the browser window. Never go through an indirect link.
5. If your log-in ID or password appears automatically on the sign-in page, disable the "Auto Complete" function to increase the security of your information.
6. Change your Internet Banking passwords (both log-in and transaction password) after the first log-in.
7. The password should be complex containing letters, numbers and special characters.
8. Create and maintain different passwords for log-in and for transactions.
9. Never to share Internet Banking passwords with others, even family members or bank employees.
10. Always check the last log-in to your Internet Banking account.

E-mail Safety Tips

- Bank/Income Tax department/financial institutions never send e-mails that ask for confidential information.
- Delete suspicious e-mails without opening them. If opened, do not click any link or attachment they may contain.

Safety Measures for online shopping

- Be very sure of the website address. Bookmark the websites that you use frequently.
- Never enter, confirm or update your account-related details in a pop-up window.
- Confirm that the website is a secure one. Look for "secure transaction" symbols.
- Shop only from reputed websites.
- Beware of online offers that require you to provide your account details "for verification".
- Get yourself enrolled for 3D Secure (Verified by Visa, MasterCard, SecureCode) service. This is now mandatory for carrying out online transactions.

Tips for safe usage of credit/debit card

- As soon as you receive the consignment carrying your card, ensure that the card in the envelope has your correct name printed on it.
- Sign on the reverse of the card immediately on receipt. Unsigned cards are invitations for misuse.
- Memorise the PIN and destroy any written reference.
- If the card is lost or damaged, it should be immediately reported to the Bank to block it instantly.
- Also report the loss of card to the local police station.
- Keep the card in a safe place
- Note the contact numbers of your bank where it is readily available.
- Ensure that the card you got back after a transaction is indeed yours as many times, cards get exchanged at crowded merchant locations.
- Ensure your card is swiped in your presence and not swiped on multiple devices.
- Ensure that your card number, card-expiry date and the three-digit security code on the back of the card are not captured in writing anywhere.
- Never give a photocopy of the back of your card to anyone for any reason.
- Do not hand-over your card to anyone, even if they claim to be bank representatives.
- To cancel the card, cut it in four pieces diagonally across the magnetic stripe and discard.
- Do not use a replacement card before the primary card is blocked.
- Don't expose the card to excessive heat or keep it close to a magnetic field.
- Destroy statements, charge slips, bank mails before disposing. Many identity theft cases take place through mail sniffing or garbage pilfering.

Tips for safe ATM usage

- Ensure that no one sees you enter your PIN.
- Never allow a stranger to assist you while using an ATM.
- Press 'Cancel' before ending your transaction and wait for 20 seconds before leaving the ATM area.
- After completing your transaction, secure your card

and count the cash before leaving the ATM area and not outside it.
- Do not leave your transaction record at the ATM. Shred it before discarding it.
- Change your ATM PIN frequently.

Tips for safe usage of electronic Cards for shopping
- Use the card with merchants that you trust.
- Never allow the shopkeeper to take your card to a different room for swiping.
- Make sure that your own debit card is returned to you after a purchase.
- After a purchase, always take your charge slip.
- Check charge slips against monthly account statements. Report any unauthorised transaction(s) immediately.
- Check your charge slips against your monthly account statements to verify your card transactions.

(b) Organisational Level:

The web offers many advantages. But it is also a very dangerous place to be in. The cyberspace is teeming with viruses and worms and hackers. If the computer terminal is not protected by a proper security system, a cyber attack, intentional or otherwise, can damage computer records and cause huge loss to the user.

At the minimum, any computer connected to the Internet should have all current patches of its operating system and browser installed as well as have a personal firewall, antivirus and anti-spyware software.

A more complete solution is to take a layered approach to protect the users' privacy.

1. The user should first choose an Internet service provider or an email service that offers online (server side) virus and email filters. This will block infections before downloading them.
2. The second line of defence is to install a hardware router with a built-in firewall between the modem and the computer or network.
3. The third line of defence is to use a personal firewall, anti-spyware, anti-virus, anti-Trojan, anti-spam and anti-phishing software.

The firewall is a set of related programmes located at a network server that protects the resources of a private network from users of other networks. An enterprise with an intranet system that allows access to the Internet, should install a firewall to prevent outsiders from accessing its own private data and controlling what outside resources its own employees have access to.

There are mainly three types of firewalls in use – Proxy Server, Packet Filter, and Application Gateway. It depends on the firm to use the type most suited to its needs.

If, however, in case the most unfortunate scenario when nothing seems to work, it makes sense to have backups of at least the vital records from time to time.

Lurking Dangers

The above sections were a historical perspective on digital security. However, with the fast changing digital landscape, this section highlights the dangers posed by some of the upcoming technologies that are said to change our lives (positively / negatively!) in the years to come.

Cloud computing

Cloud computing is location-independent computing where shared servers provide resources, software, and data to client computers and other devices on demand. The concept is same as that of an electricity grid. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if it was a program installed locally on the own computer.

In simple words, the user no longer requires to purchase and store software and data in ones own computer. This reduces the hardware cost substantially, reduces the need to have expensive backups, easy and quick implementation of a job on-demand, etc.

The danger in all this is that the user has no 'total' privacy of his data. The technology infrastructure 'in the cloud' is also beyond control. Since the user does not have any direct control over his own computer files, he becomes basically handicapped if something goes wrong within the cloud.

Wireless broadband

The advent of Bluetooth, Wi-fi and Wi-max has enabled people to use high-speed computing without wires. This has revolutionised modern business and has made every employee instantly accessible.

But have you ever wondered that if wired connections can be easily hacked and tapped, what can happen when data moves through open air? Even another person sitting next to you with some basic tools can intercept and read your data.

Software as a service (SaaS)

It is sometimes referred to as 'software on demand'. It refers to all those software that are deployed over the Internet and/or is deployed to run behind a firewall on a local area network or personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, or through a subscription model.

The advantages are that the applications can be accessed from anywhere with an Internet connection, rapid scalability of operations, automatic backups and updates, besides zero payment for unused software and applications.

The main drawbacks are that as users can't modify the particular software they use, they can't control their own computing. Also, in SaaS, important corporate data gets stored and controlled by third parties, making a big security risk for users.

Mobile computing

Laptops, Internet-enabled mobile phones, netbooks, and now tablet PCs are all designed to entertain and work while you are 'on the move'. This saves a lot of time for the modern professional. But the physical act of getting your device stolen or damaged while you are on the road, creates a nightmare for the user. A small case in point is the trauma we feel when we lose our mobile phones with important contact numbers and messages. This is apart from the risk of working through a wireless connection, as already mentioned above.

Online filing of tax returns

Now-a-days, the Income Tax department encourages taxpayers to file their income tax online either through its own portal or through some service-providers like taxsmile.com. These sites claim to have 128-bit encryption Secure Sockets Layer (SSL) technology and secured servers. But these are not foolproof systems. Also, there are chances of making wrong filings and filings through malicious websites that claim to be authentic ones.

Geotagging

Another emerging concern is the increasing use of GPS-based location services. This technique called geotagging embeds location-coordinates of an individual or place into pictures, videos and status updates that are then shared on open platforms like Facebook, YouTube and the like. Geotagging allows users to locate nearby commercial or entertainment destinations or even to find ones way through an unknown place through virtual maps. This facility, in spite of some advantages, allows strangers to track the movement of the user on a real-time basis.

National security

The virtual space is gradually becoming the battleground of the 21st century. Governments across the world have become 'virtually handicapped' in the face of newer attacks from unfriendly countries or even from 'motivated' individuals. India must thus take adequate measures to have complete control over its digital connections. The seriousness of the matter can be gauged from the words of Dr. V. K. Saraswat, scientific advisor to the Defence minister: "We have to be vigilant and have to have our own software to ensure that our networks become invincible".

Others

The IT managers of leading companies and government agencies, in a survey titled 'State of Enterprise Security 2010' conducted for Symantec have rated the following initiatives of the IT sector as the most problematic from a security standpoint –

- Infrastructure-as-a-Service
- Platform-as-a-Service
- Server Virtualisation
- Endpoint virtualisation

Conclusion

The above sections quite clearly demonstrate the state of virtual paralysis that we are presently in. The situation is similar in India and around the world. The silver lining is the increasing level of awareness among the users about the dangers posed by the virtual world. But even then, most of the risks are not well understood by many until they get hit.

Is all this negative talk to deter the present and future netizens? Definitely not. But as we learn to swim before taking on the open water, similarly, we should first understand the contours of the digital landscape before attempting to navigate in the virtual world. Else, we are destined to become permanently virtually handicapped.

It may be quite possible that in the near future, job applications may contain a tick-box with the question – 'Are You Virtually Handicapped?'

References

1. *Carl Bagh (2010), "Face ban or ease encryption code: India tells BlackBerry maker", July 29.*
2. *Debashis Kundu (2009), "Information technology: Concepts and Applications Simplified", Lakshmi Prakasani.*
3. *Editorial (2010), "Cyber-security", Business line, Jul 03.*
4. *ET Bureau & Agencies (2010), "Ratan Tata files petition in SC on Nira Radia tapes", Nov 29.*
5. *http://www.icicibank.com/*
6. *http://www.rsa.com/*
7. *http://www.wikipedia.com/*
8. *Our Bureau, (2010), "Internet users concerned over online security: Survey", Business Line, Jan 20.*
9. *SiliconIndia (2009), "Banks should enhance online security: RBI", July 21.*
10. *Thomas K. Thomas (2010), "India goes on the offensive in cyber warfare", Business Line, Aug 04.* ■