SENATE OF PAKISTAN

Promoting Pakistan's Defence through
Development and Democracy

Cyber Security Manual for Journalists

2013

"There were people in news organizations who didn't recognize any unencrypted message sent over the Internet is being delivered to every intelligence service in the world. In the wake of this year's disclosures, it should be clear that unencrypted journalist-source communication is unforgivably reckless." – NSA Whistleblower Edward Snowden.

"Privacy is a precursor to freedom. If you don't have privacy, you don't have freedom." – Lance Hoffman, Head of the George Washington University Cyberspace Security Policy and Research Institute.

Contents:

From the Chairman's Desk

It gives me great pleasure, in my capacity as Chairman, Senate Defence Committee, to launch this maiden publication for the first Defence Reporters Forum media training workshop. This is one among several new initiatives that the Senate Defence Committee has taken in the recent past.

We have always maintained that defence and national security have to be redefined in these changing times so that the approach is both transparent and inclusive, particularly the civilian stakeholders and the media together with parliament are primary stakeholders.

It is in this context, the Senate Defence Committee was the first institution in Pakistan to take up cyber security as a major issue to national security among the new non-conventional threats that have emerged. The Senate Defence Committee started up by holding the first ever Cyber Security seminar on July 8, 2013 in cooperation with the Pakistan Information Security Association (PISA) and as a result of our efforts, the Senate Defence Committee announced the first ever Cyber Security Task Force under the leadership of Mr. Ammar Jafri.

With this media training workshop, we are going a step further by actively involving the media as not just a stakeholders but as a partner in our ndeavor on Cyber Security because media would always be the first line of defence in this battle.

I am grateful to one of our most experienced and professional journalists Syed Baqir Sajjad, for his technical advice for this initiative and also to our partner in this regard, Konrad-Adeneur-Stiftung.

I have no doubt that this training manual, which is the first of its kind in Pakistan, will prove invaluable to save media professionals and even the lay persons as they try to comprehend this huge challenge to our national security.

We would also appreciate any feedback or comments from those who read this training manual and who attend our media awareness workshop. I would also urge all our readers and participants of the seminar to visit our website:

www.senatedefencecommittee.com.pk.

Senator Mushahid Hussain Sayed
Chairman
Senate Committee on
Defence & Defence Production

Konrad Adenauer Stiftung

About Konrad-Adenauer-Stiftung

Freedom, justice and solidarity are the basic principles underlying the work of the Konrad-Adenauer-Stiftung (KAS). The KAS is a political foundation, closely associated with the CDU party. As co-founder of the CDU and the first Chancellor of the Federal Republic of Germany, Konrad Adenauer (1876-1967) united social, conservative and liberal traditions. His name is synonymous with the democratic reconstruction of Germany, the firm alignment of foreign policy with the trans-Atlantic community of values, the vision of a unified Europe and an orientation towards the social market economy. His intellectual heritage continues to serve both as our aim as well as our obligation today.

In our European and international cooperation efforts we work for people to be able to live self-determined lives in freedom and dignity. We make a contribution underpinned by values to helping Germany meet its growing responsibilities throughout the world.

We encourage people to lend a hand in shaping the future along these lines. With more than 70 offices abroad and projects in over 120 countries, we make a unique contribution to the promotion of democracy, the rule of law and a social market economy. To foster peace and freedom we encourage a continuous dialog at the national and international levels as well as the exchange between cultures and religions.

Human beings in their distinctive dignity and with their rights and responsibilities are at the heart of our work. We Human beings in their distinctive dignity and with their rights and responsibilities are at the heart of our work. We are guided by the conviction that human beings are the starting point in the

effort to bring about social justice and democratic freedom while promoting sustainable economic activity. By bringing people together who embrace their responsibilities in society, we develop active networks in the political and economic spheres as well as in society itself. The guidance we provide on the basis of our political know-how and knowledge helps to shape the globalization process along more socially equitable, ecologically sustainable and economically efficient lines.

We cooperate with governmental institutions, political parties, civil society organizations and handpicked elites, building strong partnerships along the way. In particular we seek to intensify political cooperation in the area of development cooperation at the national and international levels on the foundations of our objectives and values. Together with our partners we make a contribution to the creation of an international order that enables every country to develop in freedom and under its own responsibility.

In the field of international cooperation we support the G8 Afghanistan-Pakistan Initiative, the general exchange of the Pakistani and Afghan Civil Society, and the strengthening of rule of law. Moreover, we intend to assist in the development of an economic system that takes into consideration social justice and concern for the environment. The KAS sponsors conferences, seminars and publications of its partners and conducts its own programs.

The Goal:

The purpose of producing this manual is to raise awareness among the journalists about their vulnerabilities while working online or using digital devices; and providing them with resources to plan their own security protocols for dealing with the threats that are becoming complex with the passage of time. This would importantly enable them to safely produce and share the stories with their audiences.

> Journalists everywhere need digital security skills more than ever; we will need them even more in the years to come -- Frank Smyth, senior advisor for journalist security at the Committee to Protect Journalists

The manual is by no means exhaustive and provides basic how-to that media persons can use to make themselves secure in Cyber sphere.

The threats are constantly evolving with the intelligence agencies, militants and criminals coming up with newer technologies to break into your digital defenses.

Therefore, the readers should keep themselves updated by consulting other resources on Cyber security as well.

Assessing your vulnerability:

It is a well-known fact that journalists are confronted with threats while working online and/or using digital devices.

According to the press freedom watchdog – Committee to Protect Journalists (CPJ) – digital attacks and cyber-surveillance are increasing at "an alarming rate".

The CPJ notes that "Authorities in countries from Ethiopia to Colombia have accessed reporters' telephone, email, and text conversations. Government players aren't the only ones who use digital surveillance and sabotage; large criminal organizations increasingly exploit high-tech opportunities. Opportunistic or 'patriotic' computer criminals also target journalists working with valuable or controversial data."

Are you at risk?

1. Do you live in a region affected by conflict?
2. Does the government use different measures to restrict critical reporting?
3. Is internet censorship practised in the country?
4. Is corruption prevalent in the country?
5. Are human rights abuses frequent?

If the answer to anyone or more of the above questions is YES, it implies that you could be at risk because of your profession.

Pakistan is considered as one of the most dangerous countries for media persons and has been ranked 8th on CPJ's 2013 Impunity Index that spotlights countries where journalists are slain and the killers go free. Meanwhile, on Reporters Without Borders Press Freedom Index 2013, Pakistan stands at the 159th rung among the 179 countries that were ranked.

The two rankings together give a somber reading of the government's approach and plans for media freedom.

According to the watchdog, journalists in Pakistan "face an astonishing array of threats, not only from militants and warlords but also from military, security, and government officials".

Meanwhile, a study on digital security by Internews, a non-governmental organization that works for independent media and access to information, reveals that three quarters of the respondents in the survey claimed to have been harassed because of their work. However, these concerns about the security were primarily about their physical well-being with little or no attention to the emerging threats in the Cyber sphere and while using digital devices.

> Correspondents have been subject to well-crafted, spear-phishing attacks in Asia. Foreign correspondents in the Middle East have had their emails intercepted leading to potentially fatal consequences for their sources in Syria. Within the United States, journalists covering the intelligence beat have had their own email traffic with different sources cited in federal government subpoenas; the journalists themselves have also been served with federal subpoenas themselves and have become targets of criminal investigations.
> News organizations of all kinds have been subject to massive denial-of-service attacks. Other outlets have been besieged by penetrating cyber-attacks designed to either steal information or corrupt it.
> Yet, individual journalists. along with newsrooms and even journalism schools have been slow to even address digital threats, let alone take them seriously. -- Frank Smyth, senior advisor for journalist security at the Committee to Protect Journalists

The participants of the Internews survey, expectedly, said that most of them were unaware of the security risks they could face while working online like email interception and data theft.

The Internews report titled 'Digital Security and Journalists – A SnapShot of Awareness and Practice in Pakistan' noted that journalists face special security threats, but do not take

their digital security seriously and that they need to be made to understand how digital security breaches could threaten their physical security.

Even as the physical security of the journalists remains paramount, remaining unprotected in the digital world could also put your most cherished treasure – 'the source' at serious risk. Not only that, sources possessing quality information would not be comfortable in sharing that with you until they are sure that you are cyber-secure.

What are the risks?

The starting point for becoming digitally secure is to identify the elements, who could possibly steal your data and harm you and your sources; their motives and the tactics they may employ for achieving this goal.

While in Pakistan many journalists are oblivious to the digital threats, the few aware of the issue do not fully comprehend the seriousness of the matter. Participants of Internews survey believed that digital security was about keeping their computers safe from internet viruses. For that they thought, use of good anti-virus software was a useful remedy.

Another fallacious notion found commonly among the journalists is that they have nothing to hide since their professional work is quite open and transparent. This is not the right way to look at the things. At times even your ordinary socializing mails may be of great value for those prying on you.

The problem is that these attacks on digital security are difficult to detect and one may unsuspectingly fall victim to them. Moreover, damage once suffered is irretrievable.

It is, therefore, important to identify what has to be protected based on assessment about what could be potentially important for the cyber-spies and criminals. It could be your personal information, your contact list, your conversations/emails and the information on your disks.

Who could harm you?

As CPJ says Pakistani journalists face a wide array of threats, the risks can come from number of places. Therefore, it is important to be alert to all those, who are likely to be affected by your work.

The government, the military, and their spy agencies are normally at the top of any list of those likely to be snooping. However, now terrorist groups and criminals are increasingly resorting to cyber-surveillance.

The threat source has got diversified because the surveillance software and equipment once available only with the most well equipped intelligence agencies is now freely available in the market and is inexpensive. Someone with basic technical skills can use these software and devices to eavesdrop on others.

Once you are done with identifying the information that has to be protected and the potential attackers, the next step in planning your security protocols is to think about their likely tactics. This could be anything from physically seizing your system to quietly poring over all your emails and other data exchanged through your digital devices depending on the level of sophistication available with the attackers.

Unlike yesteryears, when journalists could see someone stalking them, in today's digital world your computers may have been converted into spying machines through

Communicating Securely:

As the use of internet for communication increases, so do the vulnerabilities. From emails to instant messaging, and social media and networking sites, you have countless ways to communicate. But, whether you use these platforms for personal conversations or professional work, there could always be someone electronically observing you. Therefore, your safety depends on the precautions you take.

> If you're a whistleblower, you may have a sense of who has the integrity to protect their sources, but you have no way of knowing who has the technical savvy to be able to use the tools necessary to engage in secure communication – Cato Institute research fellow Julian Sanchez.

Communicating in a secure way is important to:

a. Protect yourself.
b. Keep the identity of sources confidential.
c. Keep the identity of whistleblowers secret.
d. To remain ready for working in potentially hostile environments.

This can be done by:

i. Using secure internet connections.
ii. Keeping computers clean of all spyware, malware, viruses, Trojans etc
iii. Keeping defenses of your devices strong.
iv. Securely storing data and creating backups.
v. Encryption of your data/VOIP calls.
vi. Keeping internet browsing anonymous.
vii. Maintaining low profile on social networking sites.
viii. Careful use of cell phones.

Internet Connection:

Your internet connection is your computer's gateway to the world of internet. Therefore, it is very important to make it secure. If left unsafe, others can piggyback (steal your internet service), access information on your computer, intercept your emails, or much worse carry out criminal activities using your connection that can put you in trouble.

In case of your personal internet connection, it is advisable to opt for wired LAN-connection instead of wireless LAN (WLAN). But, if using WLAN always have WiFi Protected Access 2(WPA2) encryption because everything else can be compromised.

Moreover, keeping the computer always connected to the network makes your system more susceptible to attacks.

Your wireless security can be bolstered by taking the following steps:

Access Point (Router):

Change the default SSID– SSID stands for "service set identifier"or the names of a wireless local area network (WLAN). Create a strong SSID; something that cannot be easily guessed and disable the "Allow broadcast of name" from broadcasting the SSID.

Change the default password on the router/access point. By changing the default password, it will be more difficult for the intruder to make changes and control your wireless network.

Check if the remote access is enabled or disabled. The remote access, if enabled, gives you the ability to access the router remotely using the web browser such as Internet

Explorer:

Locate the router/access point near the center of the building– If it is located near a window, there will be a stronger signal emanating from the building, which makes it easier for an intruder to locate your wireless network.

Disable the wireless connection when not in use. Turning off your wireless connection when not in use will limit your exposure to threats and intrusions.

Computer Settings:

Disable the 'Automatically Connect to Available wireless network' setting on your laptop or desktop.

Working At A Hotspot:

Hotspot is a public network that offers paid or free internet access. While using a public network it is recommended to:

1. Turn off File and Printer Sharing
2. Make sure that you're connected to a legitimate access point. Be aware of your surroundings. Don't let anyone see what you are entering in your computer.

The Computer:

Personal computers/laptops are considered as a weak link in the cyber-security regime because they contain huge quantities of data.

A system that has not been suitably protected is vulnerable to be infected by viruses, Trojans, malware, keyloggers or worms. Infected systems could render their owners susceptible to identity theft, stalking, harassment, and legal action for crimes perpetrated by hackers.The other danger is that of your system being physically seized.

> If you look at any of the breach reports, most of them still come through the simple things. Doing the simple things well, and proving that you've done them, is still the biggest challenge - Head of security strategy at NTT Com Security, a global cybersecurity firm, Garry Sidaway for Guardian.

Computer security is about protecting the system you use and the data it contains by reducing the risks to availability, integrity and confidentiality of the information that you utilize through your computer.

Computer security is part and parcel of usage of the system and is not something that can be dispensed with. It's all about being careful while working on the system. Security is needed for preventing attacks, detecting any intrusion that might have occurred and responding to unauthorized actions.

Essential elements of computer security involve physical protection of the system, reducing the risk of malfunction, preventing unauthorized access and encryption of the important data.

A virus, Trojan or worm can harm computers and networks. These may also be used to retrieve information from your computer for example, passwords and security access codes

and deliver them to the attacker.

Keyloggers, if installed on your system, can collect all the keystrokes you make on your keyboard and the screenshots that you take and transmit them back to the person targeting you. Keyloggers particularly affect the security of encrypted drives.

Meanwhile, spyware, if installed on the computer, gathers personal information from the computer and relays it back to another computer, generally for advertising purposes. Spyware normally gets installed in your system after you download freeware and shareware programs. Spyware besides slowing down computers make them susceptible to attacks by hackers.

What can be done?

Physical security measures:
Physical security needs to be carefully considered, but still this aspect does not get much attention. The equipment may be physically seized, stolen or damaged for gaining access to the information that may be stored in it or preventing you from using it.

The steps needed to secure a system would depend on your evaluation of the threats. You need to ask yourself how easy would it be for anyone to access your computer and walk away with the device or steal the data, secondly are you moving into or working in a potentially hostile environment?

You can accordingly work out your response, which can be locking-down the equipment, to protecting your confidential data in a separate storage device eg a USB flash drive or in cloud storage.

Moreover, keep the system switched off when you are away from it and don't insert other's drives into your system.

While working always beware of prying eyes.
When replacing your computers, special care has to be given to ensure that deleted files have been discarded. It has to be remembered that deleted files are not destroyed permanently and can be retrieved. To permanently erase data from your system/hard drive, you would need software that overwrites the deleted space eg BleachBit, Webroot Window Washer. The process is called bleaching.

Fire, natural disasters, and fluctuations in voltage are other most significant threats that can damage computer equipment and/or the data held on it.

Strong passwords and user authentication:
Besides, physically protecting the equipment, the other element of computer security is limiting unauthorized access to the system or the data stored on it. This can be done by configuring your devices to require password or PIN for unlocking it. Passwords should be set separately on the BIOS and Windows.

The passwords you choose should be strong preferably containing a mix of random upper and lower case letters and numbers and shouldn't be something common that others can guess. Computers nowadays also have biometrics option. It is advisable to use "multi-factor security authentication" - An approach that requires presentation of two or more of the authentication factors so that even the determined thieves feel challenged in breaking into it.

Trick the keyloggers: When typing password always type few random letters in-between elsewhere on the windows. This would help dodge key loggers, but, the bad news is that there are screen loggers also.

Storing Data:

Keep minimal data on your system. Save all confidential data on USB drive or store the data in cloud on services such as Google documents.

File Encryption:

A useful way for further securing the confidential data is through file encryption, which can be done by using software such TrueCrypt, BitLocker or FileVault. Encryption can protect specific files, the whole drive or portable storage devices eg USB.

Even if you do not go for using dedicated encryption software, you may at least set password on your important files, which is a fairly easy procedure while using Microsoft Office or OpenOffice.

File encryption would work even if your equipment falls in wrong hands.

Anti-virus and firewall:

It would be reckless to have a computer, which is connected to internet, without antivirus software.

A range of Norton antivirus software is available from www.symantec.com, but good anti-virus is also available for free. Antivirus can be had for free from Microsoft Security Essentials.

Computers connected to internet should additionally have firewall protection. Firewall on personal computers is software based.

Both antivirus and firewall have to be regularly updated so as to be effective.

Creating backup of files:
Creating backup of the data is another way of securing the data that could be lost due to hardware failure, files getting corrupted or other reasons. The choice of storage media and its security is equally important.

Use original software:
Don't use pirated copies of software instead always go for the original copies. Pirated copies may contain viruses and also increase your software vulnerability. If original copies are unaffordable, then instead of using pirated copies go for free and open source options – OpenOffice instead of Word; Firefox or Chrome browsers instead of Explorer; Ubuntu instead of Windows.

Be careful while working online:
Don't open un-scanned email attachments or links in the email even if they are coming from a source known to you. Before opening email attachments preview them with Google Preview if you are on Gmail or check them with VirusTotal.com.

Keep an eye on processes running on your computer:
Take a look at the running processes for any key loggers and other suspicious processes you have never heard of before.

Remember that you yourself are your system's best protection. For this you need to change your habits.

Using a shared computer:
Avoid using public computers or systems that are not owned by you because working on anything that you are not sure about is not secure even if it has SSL and other similar security certifications. Such systems usually have keyloggers, false security certificates and monitoring software. Therefore, the best precaution while working from

a public network/computer is never to log on to your personal accounts or post something from there.

However, if there is no other option, the standard advice is

a. Never save your log on information and disable, if any, auto login save options before starting browsing or logging in to your personal accounts

- ✓ Click Tools and then click Internet Options.
- ✓ Click the Content tab, and then click Settings, next to AutoComplete.
- ✓ Click to clear the check box for User names on passwords and forms.

b. Always log out instead of just closing the browser.

c. Clear usage history from the browser that you used and delete temporary files.

d. Don't enter sensitive information like credit card numbers or other similar details.

Following these protocols does not make you completely safe except for slightly decreasing your vulnerability.

Browser:

Web browsers enable you to use internet. The browsers are a primary target of the attackers for undermining your digital security since most of the threats come through internet.

Browser hijacking is a type of online fraud. Scammers use malicious software (malware) to take control of your computer's Internet browser and change how and what it displays when you're surfing the web. – Microsoft Safety and Security Center.

A browser that does not have enough security features would allow spyware or malware to be installed on your computer without you even getting to know about it.

How does this happen?

When you visit a website using an insecure browser 'drive by download' is achieved without your knowledge using features existing in the browser that enable scripts to run. This drive by download installs malware and spyware infecting your computer.

To check if the browser you are using is up to date visit https://browsercheck.qualys.com/ and scan scan your browser. It would point out vulnerabilities of your browser. In general practice, following steps may be taken for keeping your browser safe:

- Keep your browser up to date and enable auto update. The browser providers regularly update the browsers fixing their vulnerabilities. Therefore, an updated browser is your best security against an attack.

- Disable adds-on (plug-ins), pop-ups and phishing sites. The more adds-on you have, the greater is the risk. Therefore, retain minimum number of adds-on, but keep them updated.

- Set your browser for not storing passwords.

- Disable third party cookies. Cookies are mostly harmless storing information for you. However, some of them could be used to track your browsing habits for those spying on you. Therefore, use an anti-spyware program that scans for so-called tracker cookies; and cookie management programs. Moreover, use plain text email display instead of HTML to avoid tracking cookies and files embedded in emails.

- Use browsers that are compatible with Transport Layer Security (TLS) or Secure Sockets Layer (SSL) cryptographic protocols.

- Be sure to always use HTTPS in browser connections. The web address should begin with 'https://'. The 's' stands for 'secure'. HTTPS attempts to make a secure connection to the websites. If it fails to make a secure connection, it changes to unencrypted HTTP.

- Look for a padlock symbol in the address bar of the browser.

- It is advisable to set Firefox as the default browser because of its better security features.

- The specific settings that you would require to make for different browsers are
  - Install Noscript add-on for Firefox
  - Disable Java for Safari
  - Set up security zones for Internet Explorer.

Anonymous Browsing:

Anonymous browsing is surfing the World Wide Web while keeping your IP address and other personal details undisclosed.

Why to hide?

Anonymous browsing is useful for protecting online identity, avoiding surveillance and accessing website that could have been blocked by authorities. It would also conceal your current whereabouts.

Anonymity can be achieved by using various anonymous or proxy webservers that act as a curtain between you and the websites that you are accessing. This can be done either through the use of a Virtual Private Network (VPN) or free anonymizing services like the Tor (The Onion Router).

Tor introduces itself as a "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security…. For most uses, Tor provides the best available protection against a well-resourced observer."

Reporters Without Borders recommends the use of Tor for privacy and security.

> Tor is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor works by sending your traffic through three random servers (also known as relays) in the Tor network, before the traffic is sent out onto the public Internet. – Reporters Without Borders

All that you have to do is to download Tor Browser Bundle and you are done. The browser bundle is readily configured and patched for better anonymity.

When using Tor, it is important that additional addons and

Online Identity:

The most appropriate way to protect yourself online is to keep a low profile. It may be quite unlike of journalists, who prefer to have a conspicuous presence, but doing so would not only protect you from harm, retribution or harassment, but could also make it easier for you to reach out electronically to your sources for getting information.

The personal information that one normally shares online may include full name, address, contact details, date of birth, parents'/siblings' names, spouse identity.

The more the information about yourself you put online, the more you put yourself at risk.

This information could be stolen when:

- You share personal details over the phone or internet
- The information stored on the computer is illegally accessed by others
- Your email or accounts on social networking sites are hacked

Knowing your personal information makes it much easier for spies and cyber criminals to compromise your email, social media or other accounts that you may have on the internet for using various resources.

Simple things that you need to do for keeping yourself safe:

Protect your computer:

You need to have firewall and software for protection from virus, malware and spyware protection installed on your computer. These must be regularly updated and scan the files on the computer frequently.

Avoid using your real identity:

Don't use your real name or address if not essential. Moreover, use different account names when setting up multiple accounts. Try to be as general about your personal information as you can.

In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

In many ways, this was all my fault. My accounts were daisy-chained together. Getting into Amazon let my hackers get into my Apple ID account, which helped them get into Gmail, which gave them access to Twitter. Had I used two-factor authentication for my Google account, it's possible that none of this would have happened, because their ultimate goal was always to take over my Twitter account and wreak havoc. – Journalist Mat Honan writing on WIRED on how he fell victim to attacks by hackers.

Don't access personal information from a shared computer or shared network

Don't login to your email or other accounts from a shared/public computer or through a shared wireless network because the passwords can be retrieved.

Know what you're sharing:

GPS information might be disclosed when you post photos or videos. So be careful while doing so.

Be vigilant:

Do not respond to emails asking for your personal information by using the 'reply' button even if coming from what looks like a trusted source. Reply by creating a new message and using address from your contact book, but only after confirming from the known sender if the information had been requested.

Emails:

Email is one of the most important means of communication for the journalists. From routine press releases to regular interaction with the sources, email has become the backbone of any journalist's daily communication replacing surface mail, telephone calls and face to face meetings because of the convenience it provides.

But, with the growing reliance on email, issues related to its usage have also come up and email security is one of the major concerns today.

What's email security?

The principles of email security are:

Confidentiality: The email sent over a particular service is protected from unauthorized access.

Integrity: It implies that the email would be safely and securely delivered to the intended recipient without having been tampered or withheld by an unauthorized person/entity.

Availability: It pertains to the availability of the services of the email service provider.

What are the threats?

Viruses:

Viruses top the list of threats to email security. At times contained in attachments with the emails, the viruses can destroy data, affect your system and can also bring down the entire mail service.

Spam:

Also known as junk mail, Spam is another major threat to email security because of the high volume delivered to the inboxes that may affect the availability of the system, but could also contain viruses, malicious code, and fraudulent solicitations for private information.

> The email from the bank looked innocent enough. It was from paymentsadmin@lloydsplc.co.uk, and Sarah Flanders, a 35-year-old charity worker from north London, didn't think twice about opening it. But the email contained software that immediately began encrypting every file on her computer – from precious family photos to private correspondence and work documents. In just a short time all her files were blocked, and then a frightening message flashed up on her screen: "Your personal files have been encrypted and you have 95 hours to pay us $300."
> Flanders is refusing to pay, but fears her personal files are now lost forever. She is one of the lastest victims of a particularly malacious piece of "ransomware" called CryptoLocker, which is estimated to have targeted nearly 1m computers over the past month alone. – Guardian Oct 19, 2013

Phishing:

Phishing or identify theft, is done by cyber criminals through installing malicious software on your computers or making you to handover over your personal details to them. The attackers lure their victims to spoofed websites and download something from there or trick them into giving their back account details, credit card numbers or personal ID.

A phishing email may look like this:

Yahoo! Snippet unavailable
To inbox@yahoo.sg
Oct 15

YAHOO! MAIL

Your two incoming mails were placed on pending status due to the recent upgrade to our database, In order to receive the messages Click here to login and wait for responds from Yahoo.

We apologies for any inconvenience and appreciate your understanding.

Regards, Yahoo Group.

Snooping / Interception:

Eavesdropping is a hard fact that has been long known, but recent disclosures have confirmed the extent of interception of emails by intelligence agencies making this aspect a major threat to email security. Interception of 13.5 billion emails just from Pakistan in March 2013 by United States' NSA shows how serious is the threat.

Basic Security procedures:

1. Use HTTPs secure connections. Always use HTTPS:// and not HTTP:// .
2. Don't download attachments with the email even if sent by a known source. First view the attachments using "view" option instead.
3. Don't click on the links present in an email.
4. Set your email view settings as text instead of HTML.
5. While replying try to create a new mail and add the address from your address book instead of just hitting the reply button.
6. Keep your official and private email addresses separate.
7. Treat your e-mail address as important private data and only share it with those whom you know or trust. Don't publicize them unnecessarily.

Email Encryption:

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it." – Edward Snowden.

Many email services offer secure end to end communication through encryption, but NSA revelations have shown that spy agencies have successfully cracked HTTPS and Secure Sockets Layer (SSL) encryption technologies. Therefore, it is advisable to use 'public key cryptography'. For this purpose open source GNU Privacy Guard (GPG) or Symantec's Pretty Good Privacy (PGP) are good options and they can work with most of the email services.

PGP involves use of two keys a public key and a private key. These keys can be generated using tools or services that are available online.
The keys may be a bunch of letters and numbers that would help you encrypt and decrypt the messages.

How does it work?

The sender composes the message and encrypts it with the public key before sending it. Anyone else reading the message would find it as a garbled text, but the intended recipient could decode it using the private key.

(For detailed procedure of creating encrypting emails visit http://www.gpg4win.org/doc/en/gpg4win-compendium_5.html)

N.B. All your efforts for securing your communications would be futile if the person with whom you are corresponding is not complying with the security procedures and is keeping his/her mails unsecured.

Steganography:

Steganography is concealing a sensitive or confidential message behind something else like images, text files so that no one other than the sender or the intended recipient knows that it exists. It takes cryptography a step further in that an encrypted message can be hidden or made part of some other file. It uses digital media files or network protocols as a carrier in which secret data is embedded Anyone scanning your data will fail to know it contains encrypted data.

Steganography can be done by using programs like Openpuff, OurSecret or QuickStego.

The procedure for Steganography given by OurSecret:

1. Install Our Secret (download). (Can be downloaded from http://www.securekit.net/oursecret.htm)

2. Hide file.

Let's hide a picture (Jennifer.jpg), just for example, you could also add a file or a message) into a carrier file (carrier.jpg).

Step1: Select carrier.jpg as your carrier file.

Step2: Add Jennifer.jpg.

Step3: Specify a password (Here we enter "friends").

Then we get the result file (result.jpg) which hides Jennifer.jpg. As you can see, it exactly looks like carrier.jpg! No one knows Jennifer's picture is in it except you!

Jennifer.jpg carrier.jpg result.jpg

It's amazing, isn't it? Download these pictures and give it a try!

3. Unhide File

- Select result.jpg.
- Enter the password "friends".

You retrieve Jennifer Aniston's picture (Jennifer.jpg) from result.jpg. Just so easy!
Other Steganography programs may have slightly different procedures.

Spammimic:

Spammimic is encrypting a short message into spam without anyone getting to know that you are sending encrypted messages. There is so much of spam going around on the web that someone would pay attention to a message that apparently is spam.

Its really simple and hassle free.

1. Visit the website www.spammimic.com
2. Enter your message for example "You are invited to Workshop on Cybersecurity for Journalists" into the encode bar and press 'encode'.
3. A coded message would be generated, which looks like this:

"Dear Friend ; Especially for you - this red-hot announcement . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 2216 , Title 9 ; Section 303 ! THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich within 41 days ! Have you ever noticed more people than ever are surfing the web & how many people you know are on the Internet ! Well, now is your chance to capitalize on this . We will help you SELL MORE and increase customer response by 150% ! You can begin at absolutely no cost to you ! But don't believe us . Ms Ames of Georgia tried us and says "I've been poor and I've been rich - rich is better" . We assure you that we operate within all applicable laws !"

4. Copy the coded message into your email and send it.

The recipient would copy this message and again paste it on www.spammimic.com for decoding and get the original message.

Instant Messaging:

Much like emails, messaging or chat using Windows Live Messenger, Yahoo, or other services is likely to be intercepted because most of it is unencrypted.

The good news, however, is that like PGP and GPG for encrypting emails, you can use 'Off the Record (OTR)' feature for private conversation over instant messaging.

Benefits of using OTR are

1. Encryption: Messages are encrypted and cannot be compromised.
2. Authenticity: The person on the other side is the same, who you intended to correspond with.
3. Confidentiality: The messages cannot be read other than the person for whom they are intended.
4. Secrecy: Conversations are secure.

OTR plug in can be downloaded for use with services like Yahoo and also with universal chat client Pidgin that can work with almost all networks – MSN, Yahoo!, Google, Jabber, and AIM.

Gmail's Google Talk's "off the record" is different from OTR because it is not encrypted the way OTR does and are saved on Google servers and can be displayed at a later time.

Another issue with Google's "off the Record" is that if the person with whom you are corresponding is using some other client then your conversations can be logged.

Google's "off the record" is not as secure as you would like it to be.

Social media sites:

Journalists have been using social media tools – blogs, wikis, Twitter, Facebook, …. – as an additional source of information and opinion on issues of interest to them, but at the same time this has made them more vulnerable to cyber stalkers, snoops, trolls, identity thieves, hackers, spammers and other criminals.

The beginning point for safe use of social media tools is to know the risks. The profiles that one builds on social networking sites could be too much revealing. This information could be used to harass, harm, or even tarnish your reputation. It could also be exploited to plant spyware in your system or send spam mail from your account.

> Be aware of the personal material you or your family post to Facebook or other social media sites. The people who wish to intimidate you are likely to seek out everything published online not only about you, but about your family as well. Do not share information about your family's daily schedule or vacation plans, for example. Take care in publishing photos or disclosing information not otherwise public. – Committee to Protect Journalists.

The hackers break into your accounts by using 'Forgot your password' option, which leads to security questions like date of birth, schooling, parent/spouse's name, hometown. The hackers intending to break into your account can search for the needed information from the profiles that you display on your social media pages.

Moreover, the opinion/comments expressed on these forums can hurt your future prospects as well.

Online conversations and the personal data that you publish are there to stay no matter you update that or delete them.

Overview of risks on different social sites:

Facebook

- Privacy issues: Personal information is maintained by the site and is easily accessible to others. Every bit of data is stored and sold/shared.

Blogs

- Disclosure of critical information
- Quality control: material posted imprudently could affect your reputation

Twitter

- Privacy issues: All tweets are public Message could be misinterpreted or distorted because of content limitations.

YouTube / Google Video

- Privacy issues: YouTube, though currently inaccessible in Pakistan, keeps track of personally identifiable information.
- You may be implied to be endorsing commercial products and offensive material.

Flickr

- Unrestricted access to your collection may allow others to comment on them or misuse them.

While using social media tools:

1. Be careful about what you post. Think twice and use common sense before posting anything.
2. Be prudent about status updates and refrain from disclosing your location at any particular time.

3. Exercise caution while opening links shared in message on social media.
4. Don't allow the social networking site, you are using, to access your email account and contact list.
5. Never trust received messages to be originally coming from the source they are showing because the source account could have been compromised. When in doubt or when you notice some unusual message always confirm its authenticity using an alternate method of communication.
6. Invitation from friends and acquaintances to social media sites may be from scammers.
7. Don't use links to access social media sites because they may lead you to fake sites, instead always type the address in address bar by yourself.
8. Be vigilant while accepting 'friends' requests and check the profiles of those making the requests. It is preferable to add only those as 'friends' that you personally know because making someone a friend online enables that person to see your personal information and posts.
9. Before using any social site assess its level of protection. Things to look for are terms of use; how public would be your profile (some sites automatically make profiles public; others set them to private by default); who are permitted to comment on your posts; whether or not the site would own your information and posts and share it with corporate sector to target you for advertisements; and how effectively the site responds to abuse complaints.
10. Keep firewall, antivirus, antispyware, and antispam software on your system updated.

Using VoIP:

"Security issues relating to VOIP have begun to surface…. But this has to be a major consideration. Chances are, you are unlikely to get hacked. But once you do, you'll never forget it." -- Christopher Kemmerer, communications expert.

Voice over Internet Protocol (or more commonly known Internet telephony) has in many ways changed telecommunications. It is the preferred option because of lower cost, flexibility and the secrecy, which it is believed to be providing. But, much like other digital technologies it too comes with security risks.

VoIP calls pass across the internet and there is a risk of communications being monitored. The risks are similar to those of emailing. VoIP calls should be encrypted or on Virtual Private Network (VPN) connection. Otherwise take precautions when entering sensitive information. –Australian Internet Security Initiative.

There are a number of VoIP services providers – Skype, net2phone, vonage, phonepoweretc – from amongst whom you can choose the one that suits your requirements. Primary considerations while opting for one of these service providers are vice quality, interoperability and latency (or the voice lag). Security seldom factors in the choice.

It is important to note that VOIP security is as important as the data security and has to be handled in the same manner.

You have to be mindful about the security concerns to avoid disruptions in service, prevent unauthorized calls and protect sensitive phone conversations and records.

Major risks are eavesdropping, hacking, phishing attacks (also called vishing), denial of service (DoS) attacks, spamming over internet telephony (SPIT), call tampering,

man in the middle attacks and the viruses/malware.

Use of softphones (the software used to make and receive calls over internet) adds to vulnerability.

Therefore, it is vital that you make your systems secure through firewalls, patching against vulnerabilities and regularly scanning your systems for detecting any intrusion. And to make your conversations secure, you would have to rely on encryption.

Firewalls are the basic protection tools that block the invasive and malicious traffic. However, the problem is that the firewalls may be good at protecting against traditional attacks, but offer little protection against targeted attacks and eavesdropping.

Encryption is a useful way to protect conversations. It works. There are number of ways to encrypt the VoIP calls. One such product Zfone is becoming increasingly popular.

Zfone can work on Windows XP, Mac OS X and Linux. Moreover, both caller and the recipient should be using Zfone. If one of them is not on Zfone, the call would not remain encrypted. The Zfone interface shows whether or not the call is secure.

Using VOIP Tunnel is another useful way for safe encrypted communication. VOIP Tunnel can also help in areas/countries that do not allow internet telephony.

Skype uses encryption, which cannot be intercepted. This made it a popular choice for those wanting to have secure conversation. But, it is not the case anymore. Skype now stores the conversations for up to 30 days and may share them with law enforcement agencies.

Journalists while making accounts on Skype or other providers should avoid giving personal details so that they are not immediately identified.

Moreover, when contacting sources, the journalists should use proxy server, so that their IP address cannot be traced.

It is advisable that while talking to sources through VOIP do not reveal your identities during conversation.

Adoption of security measures would lead to degradation of voice quality and slow the speed. However, it is a tradeoff worth making.

Cell Phone / SMS:

Mobile phones serve as the basic source of communication for the journalists in their professional work. But, at the same time the phones provide the spies and criminals, trying to target you, their best chance to get all the information that they may require about you. Remember phones leave behind a telltale trail. The phones don't just tell whom you are talking to and what you are talking, but would also disclose your location.

Whether you are using an ordinary cell phone or a smart phone, you remain at risk. The features that make the phone a smart phone in fact increase your vulnerability.

> The modern handset is a complex computer with a vast range of sensors and capabilities. Users need greater knowledge of, and training on, the capabilities of handsets today. There is a need to understand the safety and security challenges that users who live in restrictive regimes face on a daily basis. – Freedom House report 'Safety on the Line: Exposing the myth of mobile communication security'

Therefore, as a journalist you need to protect your phone from being used for spying on you and getting lost or snatched.

Single line advice for safe use of smart phones is to be smart with them.

Losing a phone is not just the loss of the device or the data saved in it, but if it falls to hostile element it can compromise entire network of your sources and their safety and security.

Signs that could indicate that your phone is being monitored:

1. Sudden drop in sound/volume during conversation.
2. Problems with dialing numbers.

3. The phone remains warm even when not in use and battery timing is reduced.
4. Placing the phone near a speaker produces a prolonged buzzing sound.
5. Phone takes longer to switch off.

Practicing some basic precautionary measures could reduce the risk:

1. Always prefer to use a pre-paid connection that is not directly registered in your name. All such connections should be bought and recharged with cash and not by using credit cards.
2. Set a password on your phone and a PIN on the SIM card.
3. Set your phone set to lock automatically if not used for a while. It should be unlocked only through entering password or PIN.
4. Update the phone regularly because updates would make your phone more secure by patching the vulnerabilities.
5. Keep the Bluetooth switched off, if not in use. And while using it keep it in invisible/hidden mode after getting connected with the desired device.
6. Preferably use an encrypted network for Wi-Fi. Exercise particular caution while working on Hot Spot (public network). Do not enter your password or other personal details when working on a public network, because by doing so you would run risk of someone else seeing your sensitive information.
7. Set your phone to require permission for connecting to a new internet network. It should not automatically connect to the available networks.
8. Get Apps and other software for your phone from a trusted source.
9. Download a security app that could prevent malicious code from running on your phone.

10. Avoid clicking suspicious links contained in emails or other messages. Small size of the phone screen makes it difficult to know if the site, whose link is given, is safe to visit.
11. Turn off the GPS, when not in use because it can tell others about your location. GPS can be used by your phone's camera to give the location of the shoot, which is called geotagging. Moreover, social media networks like Facebook and Twitter can also use GPS to geotag postings on these sites done from your phone.
12. Create a backup of the phone data on your computer, memory card or the cloud storage.
13. Keep minimum sensitive data on your phones.
14. Phones can tell your location and relay the conversation taking place near them even when they are switched off. Therefore, during the course of confidential conversation remove the battery of your phone or place them out of the room.
15. If you have changed your number/SIM to escape eavesdropping, then don't use the new SIM on the phone set that was earlier used with old SIM. Change your phone set, otherwise its IMEI number would let those tracking you know your new number as well.
16. When disposing off your cell phones, ensure that all data has been wiped off from the phone's memory.

While trying to evade snooping, it is important that the person you are calling is also following the security protocols, because he too may be a target of interception and your call could expose you.

SMS

The text messages are searchable and can be indexed. Send as few messages as may be essential.

> "There should be no doubt any more, journalism is under threat. In the light of Edward Snowden's revelations, we should see the intimidation, harassment and censorship of journalists as a declaration of war.
> Now we must arm ourselves by turning this spy technology on its head and make it work for us. Because if a journalist can't offer confidentiality then that journalist is compromised and that will sound the death knell for our profession.
> -- "Deep Web for Journalists: Comms, Counter-Surveillance, Search".