



Internet security and privacy

This fact sheet has been developed for the Consumer Education Program by the Communications Commission of Kenya. It was compiled by studying material from various authoritative sources and adopting what is universally acceptable and relevant to the Kenyan situation. The fact sheet is intended to enable Consumers have a good understanding of the issues discussed and hence empower them when making decisions regarding ICT products and services.

Introduction

Information in a computer network should be protected when on transit particularly over wireless communication media to avoid risks which relate to:

- Data security
- Privacy
- Identity theft

Securing your wireless network

Wireless devices have a number of common characteristics, the most significant being the broadcast of information using radio waves. In a broadcast system information is sent out in different directions from the transmitter, which means that any receiver within range and tuned to the transmission frequency will receive the signal.

When wireless technology is used to transmit personal information, the information has to be protected to guard against un-authorized access to the content of the signal. This risk is generally referred to as eavesdropping. Presented below are various wireless communication technologies and their inherent risks.

Bluetooth

This technology allows communication devices to communicate using short range wireless signals. Bluetooth devices are designed to operate between 2.4 GHz to 2.4835 GHz frequency band and can achieve transmission speeds of up to 1 Mbps. It can be used to link a cell phone to a headset, a keyboard or a mouse to a computer, laptop to printer etc. Security threats can occur through bluejacking, Bluesnarfing, or Bluebugging, which are defined as follows:

- **Bluesnarfing** is the un-authorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This is often characterized by access to a calendar, contact list, emails and text messages and on some phones users, can steal pictures and private videos.
- **Bluebugging** is a form of bluetooth attack where a bluebug program allows the user to take control of another person's phone. This means that the Bluebug user can simply listen to any conversation his victim is having in real

Internet security and privacy

time (eavesdropping). Bluebugging can also allow unauthorized making of calls and sending of messages from the bugged phone.

- **Bluejacking** is the sending of unsolicited messages over Bluetooth, to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers

Safeguards against Bluetooth Risks

- Ensure that all your Bluetooth devices are properly secured by using passwords other than the default passwords and also making sure that the Bluetooth function remains switched off when not in use. Always confirm that communication is secure and protected before enabling Bluetooth on any device containing personal information.

Cell phones and PDAs

These devices can not only be used for voice transmission, but also as wireless modems or web browsers. When used to transmit or store emails or instant messages they can pose a security threat, through the unauthorised access of personal information. Therefore the following security measures are necessary.

- Make sure that the devices are set up to operate in a secure manner. Security features include encryption of data during transmission, password protection and automatic data wiping.
- It is also advisable not to discuss sensitive personal or business information while in public places.

Wi-Fi

Wireless Fidelity or Wi-Fi refers to a range of technologies for wireless data networking. Wi-Fi-enabled devices such as PCs or cell phones, can connect to the Internet when in the vicinity of a wireless network. Wi-Fi has been deployed in airports, universities, bookstores, coffee shops, office campuses and private residences. Because of its low cost of implementation a wide range of individuals, many of whom are not networking experts, now use Wi-Fi devices. To avoid the risks associated with wireless networks, the following security measures need to be taken:

- Encrypt the data properly before transmission.
- Large organisations may want to use more secure Virtual Private Networks (VPN) to provide connectivity for mobile workers. Individuals or smaller organisations may use some protocols referred to as Wi-Fi protected access.

General measures for securing wireless networks

Any device found within a wireless network can serve as an illicit entry point to the entire network if it is not properly set up. This can expose entire databases of information or other sensitive personal information to access by unauthorised persons. To prevent data leakage in such situations it is vital to secure the entire network rather

Internet security and privacy

than specific devices. Taking the following measures will help further secure your wireless network:

- Encrypt the data all the time during transmission
- Use antivirus and anti spyware software and also incorporate a firewall in the network.
- Turn off identifier broadcasting or the ability for the device to send out a signal to other devices in the vicinity announcing its presence. Change the identifier of your router from the default
- Change your router preset password - this is the password to set up and operate on the router.
- Allow only specific computers to access the network
- Turn off your wireless network when you know you will not use it
- Be careful about the information you access or send out when in a public wireless network/hotspot.

Threats to privacy

Online threats to privacy include:

- Identity theft and
- Spam scams

Identity theft

Identity theft occurs when someone acquires and uses your name, PIN number, ID card number, credit card number or other delicate personal information without your permission. A common method used for identity theft is Phishing, where a fraudulent, but official-looking e-mail is sent to a user in an attempt to con that user into divulging personal and/or private information, which is then used for identity theft.

Once an identity thief has obtained someone's personal and/or financial information they can assume that person's identity (in other words - use your personal and financial information without your knowledge or permission). Then they steal your money; emptying your accounts and running up credit in your name.

Identity thieves will use your details ruthlessly. It is important to keep a close watch on your financial information because often, as that is the first place that an occurrence of identity theft will appear. Check your bank and credit card statements often for strange transactions.

Several clues present themselves when your identity has been stolen

- Mysterious financial transactions and bills for purchases you know you did not make.
- Goods or credit cards that you did not order or apply for being delivered.
- Calls from debt collection agencies about goods or services that you did not purchase.



Internet security and privacy

- Apparent redirection of mail, like utility bills and other important correspondence.
- You no longer have a good credit rating.

If personal information is inadvertently disclosed or deliberately stolen, taking certain steps quickly can help reduce the damage that can be done.

- Place a fraud alert on your credit reports and have another person look at them carefully.
- Close account - this are your accounts or accounts that have been opened fraudulently.
- File a police report - this may help should creditors request for proof of the crime.
- Notify the relevant regulatory authority.

SPAM SCAMS

Most people find unsolicited commercial emails (spam) annoying and time consuming. This type of scam poses a very huge risk to personal privacy by enabling spammers to take unfair advantage of others, especially the many users who are new to the internet and form easy prey for the spammers. However for the spammers this is an inexpensive means of reaching potential customers anonymously.

Some email users have lost money to bogus offers that arrived as spam in their in-box. Con artists are very cunning; they know how to make their claims seem legitimate. Some spam messages ask for your business details, others invite you to a website with a detailed pitch. The following tips are aimed at helping you avoid spam scams.

- Protect your personal information - share credit card information only with reputable businesses.
- Know who you are dealing with - do not engage in business with a company that will not provide you with an address phone number or its location.
- Take your time - resist any temptation to act impulsively regardless of the attractiveness of the offer and its terms. Once you hand over your money you may never get it back so act cautiously.
- Get all promises in writing and review them carefully before making a commitment.
- Disregard any offer that asks you to pay for a free gift or pay some money to redeem a free gift. If it is free it means that you do not have to pay for it.
- Many Internet Service Providers and computer operating systems offer filtering software to limit the spam in their users' email inboxes. In addition, some old-fashioned 'filter tips' can help you save time and money by avoiding frauds pitched in email.



SOME COMMON SPAM SCAMS

The 419 Email Scam

The Bait: Con artists claim to be officials, businesspeople, or the surviving spouses or children of former government officials in “Nigeria” or other country, whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or “taxes” to help them access their money. If you respond to the initial offer, you may receive documents that look “official.” Then they ask you to send money to cover transaction and transfer costs and attorney's fees, as well as blank letterhead, your bank account numbers, or other information. They may even encourage you to travel to the country in question, or a neighboring country, to complete the transaction. Some fraudsters have even produced trunks of dyed or stamped money to try to verify their claims. This email scam is also referred to as the “Nigerian” email scam

The Catch: The emails are from crooks trying to steal your money or your identity. Inevitably, in this scenario, emergencies come up, requiring more of your money and delaying the “transfer” of funds to your account. In the end, there are no profits for you, and the scam artist vanishes with your money. The harm sometimes can be felt even beyond your pocketbook as some people who have responded to “pay in advance ” solicitations have been beaten, subjected to threats and extortion, and in some cases, murdered.

Your Safety Net: If you receive an email from someone claiming to need your help getting money out of a foreign country, do not respond.

Phishing

The Bait: Email or pop-up messages that claim to be from a business or organization you may deal with — say, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information or face dire consequences.

The Catch: Phishing is a scam where Internet fraudsters send spam or pop-up messages to reel in personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization's site, or to a phone number purporting to be real. But these are bogus and exist simply to trick you into divulging your personal information so the operators can steal it, fake your identity, and run up bills or commit crimes in your name.

Your Safety Net: Make it a policy never to respond to emails or pop-ups that ask for your personal or financial information, never to click on links in the message, and never to call phone numbers given in the message. Do not cut and paste a link from the message into your Web browser, either: phishers can make links look like they go one place, but then actually take you to a look-alike site. If you are concerned about your account, contact the organization using a phone number you know to be genuine, or open a new Internet browser session and type in the



Internet security and privacy

company's correct Web address yourself. Use updated anti-virus and anti-spyware software and a firewall, which can help secure your computing environment.

Work-at-Home Scams

The Bait: Advertisements that promise steady income for minimal labor — in medical claims processing, envelope-stuffing, craft assembly work, or other jobs. The advertisements use the following baits: Fast cash Minimal work. No risk. And the advantage of working from home when it is convenient for you.

The Catch: The advertisements do not reveal that you may have to work many hours without pay, or pay hidden costs to place newspaper advertisements, make photocopies, or buy supplies, software, or equipment to do the job. Once you put in your own time and money, you're likely to find promoters who refuse to pay you, claiming that your work does not meet their “quality standards.”

Your Safety Net: Legitimate work-at-home business promoters should tell you — in writing — exactly what is involved in the program they are selling. Before you commit any money, find out what tasks you will have to perform, whether you will be paid a salary or work on commission, who will pay you, when you will get your first pay cheque, the total cost of the program — including supplies, equipment and membership fees — and what you will get for your money. Can you verify information from current workers? Be aware of people who are paid to lie and give you every reason to pay for work. Get professional advice from a lawyer, an accountant, a financial advisor, or another expert if you need it, and check out where the company is located.

Weight Loss Claims

The Bait: Emails promising a revolutionary pill, patch, cream, or other product that will result in weight loss without the need to diet or exercise. Some products claim to block the absorption of fat, carbs, or calories; others guarantee permanent weight loss; still others suggest you will lose lots of weight at lightning speed.

The Catch: These are gimmicks, playing on your sense of optimism. There is nothing available through email that you can wear or apply to your skin that can cause permanent — or even significant weight loss.

Your Safety Net: Experts agree that the best way to lose weight is to eat fewer calories and increase your physical activity so you burn more energy. Talk to your health care provider for advice on an appropriate nutrition and exercise program suited to you.

Foreign Lotteries

The Bait: Emails boasting enticing odds in foreign lotteries. You may even get a message claiming you have already won! You just have to pay to get your prize or collect your winnings.



Internet security and privacy

The Catch: Most promotions for foreign lotteries are phoney. The scammers will ask you to pay “taxes,” “customs duties,” or fees – and then keep any money you send. Scammers sometime ask you to send funds via wire transfer. Do not send cash or use a money-wiring service because you’ll have no recourse if something goes wrong. In addition, lottery hustlers use victims' bank account numbers to make unauthorized withdrawals or their credit card numbers to run up additional charges.

Your Safety Net: Skip these offers. Do not send money on the promise of a pay-off later.

Cure-All Products

The Bait: Emails claiming that a product is a “miracle cure,” a “scientific breakthrough,” an “ancient remedy” — or a quick and effective cure for a wide variety of ailments or diseases. They generally announce limited availability, and require payment in advance, and offer a no-risk “money-back guarantee.” Case histories or testimonials by consumers or doctors claiming amazing results are not uncommon.

The Catch: There is no product or dietary supplement available via email that can make good on its claims to shrink tumors, cure insomnia, cure impotency, treat Alzheimer's disease, or prevent severe memory loss.

Your Safety Net: When evaluating health-related claims, be skeptical. Consult a health care professional before buying any “cure-all” product that claims to treat a wide range of ailments or offers quick cures and easy solutions to serious illnesses.

Check Overpayment Scams

The Bait: A response to your advertisements or online auction posting, offering to pay with a cashier's, personal, or corporate cheque. At the last minute, the so-called buyer (or the buyer's “agent”) comes up with a reason for writing the cheque for more than the purchase price, and asks you to wire back the difference after you deposit the cheque.

The Catch: If you deposit the cheque, you lose. Typically, the cheques are counterfeit, but they look good enough to fool unsuspecting bank tellers and increase the balance in your bank account – temporarily. But when the cheque eventually bounces, you are liable for the entire amount.

Your Safety Net: Do not accept a cheque for more than your selling price, no matter how tempting the plea or convincing the story. Ask the buyer to write the cheque for the purchase price. If the buyer sends the incorrect amount, return the cheque. Do not send the merchandise. As a seller who accepts payment by cheque, you may ask for a cheque drawn on a local bank, or a bank with a local branch. That way, you can visit personally to make sure the cheque is valid. If that's not possible, call the bank the cheque was drawn on using the phone number



Internet security and privacy

from directory assistance or an Internet site that you know and trust, not from the person who gave you the cheque. Ask if the cheque is valid.

Pay-in-Advance Credit Offers

The Bait: News that you have been “pre-qualified” to get a low-interest loan or credit card, or repair your bad credit even though banks have turned you down. But to take advantage of the offer, you have to ante up a processing fee of several hundred dollars.

The Catch: A legitimate pre-qualified offer means you have been selected to *apply*. You still have to complete an application and you can still be turned down. If you paid a fee in advance for the promise of a loan or credit card, you've been hustled. You might get a list of lenders, but there is no loan, and the person you have paid has taken your money and run.

Your Safety Net: Do not pay for a promise. Legitimate lenders never “guarantee” a card or loan before you apply. They may require that you pay application, appraisal, or credit report fees, but these fees are seldom required before the lender is identified and the application is completed. In addition, the fees generally are paid to the lender, not to the broker or person who arranged the “guaranteed” loan.

Investment Schemes

The Bait: Emails touting “investments” that promise high rates of return with little or no risk. One version seeks investors to help form an offshore bank. Others are vague about the nature of the investment, but stress the rates of return. Promoters hype their high-level financial connections; the fact that they are privy to inside information; that they will guarantee the investment; or that they will buy it back. To close the deal, they often serve up phoney statistics, misrepresent the significance of a current event, or stress the unique quality of their offering. And they will almost always try to rush you into a decision.

The Catch: Many unsolicited schemes are a good investment for the promoters, but not for participants. Promoters of fraudulent investments operate a particular scam for a short time, close down before they can be detected, and quickly spend the money they take in. Often, they reopen under another name, selling another investment scam.

Your Safety Net: Take your time in evaluating the legitimacy of an offer: The higher the promised return, the higher the risk. Do not let a promoter pressure you into committing to an investment before you are certain it is legitimate. Hire your own accountant to take a look at any investment offer, too.



Internet security and privacy

FIGHTING BACK

Con artists are clever and cunning, constantly hatching new variations of age-old scams. Still, skeptical consumers can spot questionable or unsavory promotions in email offers. Should you receive an email that you think may be fraudulent delete it immediately.

For more information contact the Communication Commission of Kenya on the following address:

**THE DIRECTOR GENERAL,
COMMUNICATIONS COMMISSION OF KENYA
WAIYAKI WAY, WESTLANDS
P.O. BOX 14448, WESTLANDS NAIROBI, 00800**
Email: info@cck.go.ke
Website: www.cck.go.ke

Acknowledgement

This Fact Sheet was developed by Teknobyte (Kenya) in partnership with the Communications Commission of Kenya for the Consumer Education Outreach Programme.

Disclaimer

All attempts have been made in order to ensure that the information contained in this publication is accurate. However, the document is intended as guide only. Readers should ensure that they verify on their own any information contained in this document upon which they intend to rely as a basis for taking any action or making any decision. The Commission will not accept liability for the information contained in this document or for consequences of any actions taken or decisions made on the basis of the information provided.

© 2008 Communications Commission of Kenya