

Internet Safer Day

Safe Internet Surfing Practices

10 February 2009

IT Security Unit

Ministry of Information and Communication Technology

Agenda

- n Usage of Internet
- n Dangers of Internet
- n Typical Measures
- n Safe Practices

Today's Connected World ...



Usage of the Internet

- n News and Reference
- n Entertainment (movies, videos, clips)
- n Commerce (online shopping, auctioning)
- n File sharing (mp3)
- n Social Networking (Hi5, Facebook)
- n Instant Communication (email, chat)
- n Accessing Internet on Mobile Phones

Dangers of Internet

- n Online contacts through Social Networking sites
 - n Potential contact with someone you don't know (e.g. Chatting with strangers with no details on their identity)
- n Internet Content
 - n Inappropriate materials on the web (e.g. sexually explicit material, violent and disturbing images, gambling sites)
- n Commercialism on the Internet
 - n Aggressive advertising, marketing schemes and deceitful Ads
- n Online Grooming
 - n Actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child
- n Cyber Bullying

"Never heard from 'Partygirl' again..."

Real life story shared by 19 years old anonymous girl on www.sikkerchat.dk

Inbox

From: -----
To: sikkerchat@redbarnet.dk
Subject: Response to Sikkerchat website

When I was 16 I had a lot of problems with friends in the area where I lived. So I spent time chatting which was good, but after a while I had a bad experience and I stopped chatting altogether.

While chatting I met a girl who called herself "Partygirl". The first 4 sentences I remember were: where do you live, how old are you, are you alone and what are you wearing... That's how it was. We went on to talk about everything. After chatting and communicating via email for a long time we exchanged pictures, completely normal pictures.

After a month of chatting and emailing like this we planned to meet up. I thought this would be OK, and we decided to meet at the Central Station. I arrived with a rose and her picture (in order to recognize her). A man came up to me. He said something like him being her granddad. He was a little man. He looked nice. After thinking about it, I said "what do you know about me?" - And he knew too much... Then I ran away. I never heard from "Partygirl" again...

Now this is a few years ago - I'm sure, I know what his man was after. But what to do when you have been chatting online with a person that you think is your friend for more than a month?

Watch out people!

Dangers of Internet

- n Personal Information
 - n Profile or personal information could be disclosed during online conversations. Such information can lead to receiving unwanted contact from inappropriate people.
- n Pictures
 - n Posting of comments or images of oneself or others online, which may compromise the person's safety or be used as a means to bully others.
 - n Legal Aspects
 - n There may be legal consequences of copying copyrighted materials and beware of plagiarism
- n Threats (Spyware, viruses)
 - n When connected online, your computer is at risk from spyware, viruses and other invasive programmes if you are sharing files on non-regulated sites.

Typical Measures

- n **Awareness**
- n Policies & Procedures
- n Adopt **Safe Practices**
 - n Safe Internet Surfing
 - n Email Usage
 - n Spyware/Adware Prevention
 - n SchoolNet Security Guide
- n Reporting Security Breaches

Child Online Safety Action Plan

- n Endorsed by Cabinet in January 2009
- n Was elaborated in the context of the National Information and Communication Technology Strategic Plan 2007 – 2011
- n Recommendations
 - n The setting up of a Child Safety Online Website
 - n The conduct of sensitization campaigns on Child Safety Online
 - n Enactment of legislation to child safety online
 - n The elaboration of Safety Measures and best practices

Awareness

- n Be aware of internet dangers
- n Adopt safety practices
- n Attend awareness campaigns
- n Share safety tips to friends

Policies & Procedures

- n Adhere to School procedures
- n Principles & Guidelines for Internet Usage
- n School Net Security Measures
- n Child Online Action Plan
 - n Public Awareness Campaigns
 - n Safety Measures for Schools
 - n Website : <http://www.gov.mu/portal/sites/isf/index.html>
 - n Best Practices for Parents / Kids (Age Groups)

Safe Internet Surfing

- n Keep personal information private, or to a minimum
- n Make sure you keep not only your own information but other people's personal information private
- n Content posted to the Web can be copied, altered and reposted by anyone and it's very difficult to 'take back'
- n If you have created your own online space, profile or website, make sure it's set to private so that you can control who can view your thoughts, ideas, images, and videos

Safe Internet Surfing

- n Creation or posting inappropriate, offensive or even illegal content on the Internet could get you into trouble
- n Think very carefully before including a personal photograph of yourselves or your friends in your profile
- n Photos online can easily be copied, changed and used elsewhere, and can potentially stay online forever

Consequences of Posting Pictures

Case of 20 yr Joshua Lipton

- n While awaiting sentencing in a drunk-driving case where a woman was seriously injured, prosecutors obtained pictures posted on Facebook of Joshua drinking and wearing a jailbird costume for Halloween -- just two weeks after his accident.
- n Prosecutors used these pictures as evidence that Joshua was unremorseful for his actions. The result: a prison sentence of two years.



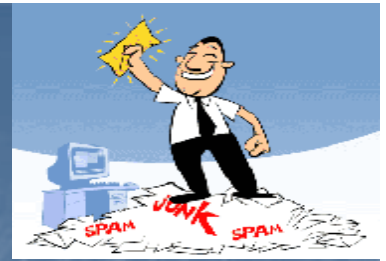
Safe Internet Surfing

- n The Web is permanent and the things you post online could come back to haunt in the future
- n Internet has become the world's electronic archive, and once photos are posted online, they can persist there forever.
- n Bear in mind that future academic institutions and employers may search for you online to see if you are the right person for them

Safe Internet Surfing

- n Meeting someone you have only been in touch with online can be dangerous. Do not agree to meet unsupervised with someone you have only contacted via the internet. **Online contacts may not be who they say they are.**
- n Phone numbers should not be given to strangers either online (in chat rooms or Instant messenger) or in real life
- n Keep your security code and pin number private and always keep your mobile hidden when on the streets

Using Email



- n Ensure you are addressing the right person prior to sending email
- n Beware of emails from unknown parties (unsolicited emails)
- n Do not open unsolicited emails
- n Never respond to unsolicited emails e.g. *'You have won \$1,000,000. Kindly send your bank details for crediting your account.'* These are scams also known as social engineering attacks

Nigerian Scam

Quick Rich Schemes

Suspicious Email

From: smithuk [mailto:smithuklo@yahoo.co.uk]

Sent: 18 February 2005 06:57

To: bodhi108@hotmail.com

Subject: WINNING NOTIFICATION: FINAL

Catching Subject Line

We happily announce to you the draw (#419) of the

UK NATIONAL LOTTERY online Sweepstakes

International program held on Wednesday 16 Feb 05.

Your e-mail address attached to ticket number:

56475600545 188 with Serial number 5368/02 drew

the lucky numbers:05-07-24-27-32-02 which

subsequently won you the lottery in the 2nd category

i.e Thunderball Jackpot.

Luring Words

Suspicious Email

You have therefore been approved to claim a total sum of **£250,000** (Two hundred and fifty thousand pounds) in cash credited to file KTU/9023118308/03.

To file for your claim, please contact our fiduciary agent: Mr. Smith Edward Email: smithuklo@yahoo.co.uk

Provide him with the information below:

1. Name
2. Address
3. Occupation
4. Marital status
5. Age
6. Country (Present Location)
7. Nationality
8. Telephone and Fax numbers.

Sophistication of Attacks

From: charles soludo [mailto:gov_charleschn2006@yahoo.com]



U.S. Department of Justice Federal Bureau of Investigation

**For Immediate Release
February 22, 2005**

**Washington D.C.
FBI National Press Office**

FBI ALERTS PUBLIC TO RECENT E-MAIL SCHEME

E-mails purporting to come from FBI are phony

Washington, D.C. - The FBI today warned the public to avoid falling victim to an on-going mass e-mail scheme wherein computer users receive unsolicited e-mails purportedly sent by the FBI. These scam e-mails tell the recipients that their Internet use has been monitored by the FBI's Internet Fraud Complaint Center and that they have accessed illegal web sites. The e-mails then direct recipients to open an attachment and answer questions. The attachments contain a computer virus.

These e-mails did not come from the FBI. Recipients of this or similar solicitations should know that the FBI does not engage in the practice of sending unsolicited e-mails to the public in this manner.

Sophistication of Attacks

AWARD FINAL NOTIFICATION:

We happily announce to you the draw (#999) of the UK NATIONAL LOTTERY,online Sweepstakes International program held on the 16th of January 2006. You were entered as dependent clients with: Reference SERIAL NUMBER: 144-66584 and Batch number BT-4478474121P.

Your email address attached to the ticket number: 74454774 that drew the lucky winnir

A handwritten signature in black ink is written over a red, slanted rectangular stamp that contains the word "APPROVED" in bold, red, capital letters.

Bonus Ball [38]
bonus. You ha
£800,000.00 |
file

Yours faithfully,
Ms.Shelley Spencer
Online coordinator for UK NATIONAL LOTTERY

to

UNITED KINGDOM

Using Email

- n Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
- n Be suspicious of all files you receive, check with the sender if you are unsure, and don't open anything sent by someone you don't know and trust.
- n Suspicious attachments must NOT be opened (files with extensions .exe, .com, .bat, .reg extensions)
- n Always keep your passwords private – Identity theft

Spyware / Adware

- n Carefully crafted programs written by attackers
- n Downloaded from Internet – often silently
- n Designed to:
 - n Gather private, personal information
 - n Create system instability
 - n Damage or interfere with legitimate applications operation
 - n Open a backdoor on infected systems
 - n Allow a spyware operator to take over an infected system

Spyware / Adware

- n Refrain from downloading unnecessary games, screensavers & other software from the Internet – they may have embedded spyware or viruses.
- n Use a regularly updated anti-spyware software
- n Protect your computer and personal files by visiting reputable sites and by installing a firewall and anti-virus software.
- n Practice safe internet surfing

SchoolNet Security Guide

- n Committee - October 2005
 - n MoEHR e-Government Unit
 - n CIB, CISD, GOC
 - n IT Security Unit
- n To ensure that security measures are taken during the implementation and operation of the project
- n SchoolNet Guide
 - n Finalised in November 2005
 - n Disseminated by e-Government Unit to all Schools concerned

Areas covered & Implementation responsibility

- n Physical Security : Head of the School
- n PC Level Security : LAN Administrator of the School (Head of IT Department)
- n Wireless Access Point (WAP) Security : MoEHR e-Government Unit
- n End User Security Guidelines : All students / users having access to a PC
- n Annexes
 - n Settings for Anti-Spyware software (Annex A)
 - n Settings for Local Security Policy (Annex B)
 - n Checklist for connecting PCs to GOC (Annex C)

Physical Security

- n To be implemented by Head of School
- n Log book to be put in place to record access and usage of Internet
 - n *Student Name, Class, Date, Time In, Time Out*
- n WAP device to be located in a tamper free area
 - n Not concealed beneath documents
 - n WAP antenna is not obstructed in order to broadcast adequate radio signal

Physical Security

- n Eating and drinking not allowed near PCs
 - n Risk of damaging equipment (e.g. keyboards)
- n Pirated and unauthorised software should be strictly prohibited
 - n May contain viruses/spyware
 - n Only original software to be used
- n PCs that access or contain sensitive data should not be connected to the Internet

PC Level Security

- n To be implemented by School LAN Admin.
- n Ensure that PCs connected to GOC have been configured as per checklist
- n PC Operating System adequately patched
 - n Configured to automatically get updates from Microsoft
- n Standard screensaver installed
- n Anti-spyware installed and configured according to the settings in the guide

PC Level Security

- n Latest antivirus and anti-spyware definitions available on the PC
- n On PCs with Windows 2000 and XP, end users to login using a restricted account and NOT with administrator access
 - n Strong password for administrator account
 - n Prevent changes in some systems configurations



PC Level Security

- n Apply local computer security policy for PCs with Windows 2000 and XP
 - n Prevents running of programs and commands from DOS prompt
 - n Blocks changes to Internet Explorer settings
 - n Prevents display of Control Panel
 - n Enable running of only required software
 - n Prevents access to LAN browsing

WAP Security

- n To be implemented by MoEHR eGovernment Unit
- n WAP device sends data through radio waves
 - n Encryption must be enabled on the WAP device to prevent unauthorised access to the data transmitted

WAP Security

- n Configure the WAP device such that only authorised PCs may connect to it
- n Use a strong password to secure access to the WAP configurations
- n Any configuration change at WAP device level must be logged and documented through a WAP device log kept at MoEHR

Reporting Security Breaches

- n In Office / School
 - n All inappropriate or illegal activity you come across must be reported
 - n In accordance with any prevailing security policy, contact the responsible person
 - n Inform your immediate supervisor
 - n Do not tamper with evidences
- n Home Users
 - n Report any case of suspected malicious attack to the Police
- n Computer Misuse & Cybercrime Act 2003
 - n Defines Offences: unauthorised access, unauthorised modification of computer material and interception of data transmitted through a computer system and electronic fraud
 - n Establishes investigatory procedures, including the power of access, search and seizure

Who is The Guardian?

You are The Guardian... engaged in a valiant battle to protect computers and information. Everyone is responsible for computer security.



- 🔒 Use strong passwords
- 🔒 Use current anti-virus software
- 🔒 Analyze incoming e-mail
- 🔒 Physically secure computers
- 🔒 Promote security awareness

*Computer Security Day
November 30th*

Please Surf Safely

Thank You