ONLINE SAFETY FOR CHILDREN

A PARENT'S GUIDE

BRUCERT

BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Brunei Computer Emergency Response Team (BruCERT) was established in 2004, and became the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei.

BruCERT is the central hub that coordinates with international CERTs, network service providers, security vendors, government agencies, as well as other related organisations to facilitate the detection, analysis and prevention of security incidents on the Internet.

Through a global affiliation with other CERTs, **BruCERT** acquires valuable information on IT security threats and shares findings on security risks detected within the nation's IT infrastructure. These findings are made publicly accessible with the objective of increasing IT Security awareness.

T +673 245 8001

F +673 245 6211

E cert@brucert.org.bn

@BruneiCERT

facebook.com/BruneiCERT

instagram.com/BruneiCERT

www.brucert.org.bn

SECURE
VERIFY
CONNECT

Secure Verify Connect is an initiative by BruCERT aimed at increasing the awareness of Internet safety and information security among the Bruneian public. We all have a responsibility to educate ourselves about cyber threats and risks to our privacy and safety. Children are especially vulnerable and need guidance so they can enjoy using the Internet safely.

www.secureverifyconnect.info

First published 2009
Second edition 2011
Third edition 2014

Dear Parents,

For most of us, Internet usage has become a necessary part of our daily routine. While there are countless benefits of being online, Internet users should educate themselves with the potential dangers that come with it. Children are especially vulnerable and need guidance so they can enjoy using the Internet safely.

This handbook is designed to help parents educate and protect their children from the possible dangers they may face while online.

CONTENTS

ONLINE THREATS

MALICIOUS SOFTWARE

Malicious software, or **malware**, is software designed to disrupt computer operations, gather sensitive information, or gain unauthorized access to computer systems. Malware includes computer viruses, worms, Trojan horses, spyware, adware, most rootkits and other malicious programs.

COMPUTER WORM

A **computer worm** is a computer program that copies itself in order to spread to other computers; often it uses a computer network to spread itself. A worm can take advantage of security weaknesses to spread itself automatically to other computers through a network.

COMPUTER VIRUS

A **computer virus** is a piece of programming-code that attacks computer and network systems through 'contaminated' (infected) data files, introduced into a system via disks or the Internet. Once infected, it attaches itself to the target computer's operating system or other programs, and automatically replicates itself to spread to other computers or networks.

ROOTKIT

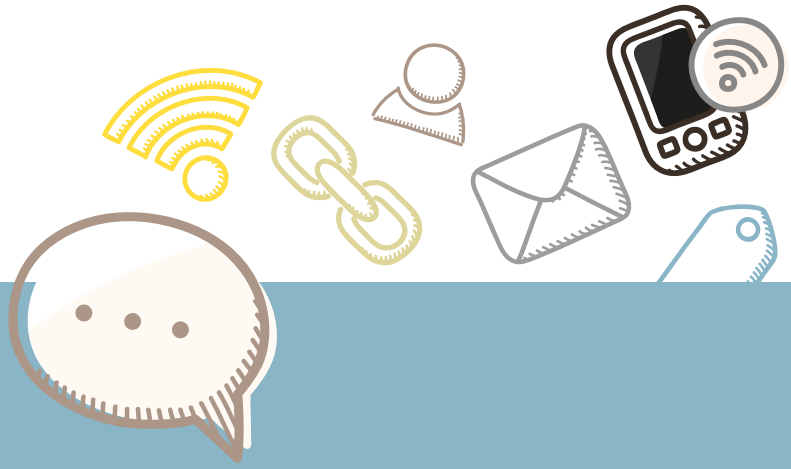
Rootkit is a software installed by a hacker, which allows the hacker to access the system at any time, even if the password is changed. It can be installed on computers and smart phones, and is normally undetectable by a normal user.

SPYWARE

Spyware is a type of program which is often secretly installed on computers that collects information about users without their knowledge.

TROJAN HORSE

A **Trojan Horse**, or **Trojan**, is a file or program that does not try to inject itself into other files unlike a computer virus and often looks like a legitimate file or program. Trojan horses can make copies of themselves, steal information, or harm the computer system.



ONLINE PREDATOR

An **online predator** is an Internet user who exploits vulnerable people, usually for sexual or other abusive purpose. Chat rooms, instant messaging, internet forums and social networking sites are common places that online predators. In Brunei, there have been several cases of rape and sexual assault involving minors who met their perpetrators online.

INAPPROPRIATE CONTENT

Some content on the Internet may be inappropriate or harmful for children, such as violent or sexually explicit material, images of child abuse, and videos that show risky or illegal behavior.

CYBER BULLYING

Cyber bullying occurs when the Internet or mobile phones are used to harm a child in a deliberate, repeated, and hostile manner such as making threats or causing embarassment. If an adult is being bullied, it is called cyber-harassment or cyber-stalking.

CYBER STALKING

Cyber stalking occurs when someone uses the Internet or other electronic means to stalk or harass an individual or a group of individuals. A cyber stalker may be anonymous and may get the help of other people online who do not even know the victim.

ONLINE SCAMS

Online scams refers to the use of Internet to make false demands to potential victims, to conduct false transactions, or to transmit the earnings of the scam to unfavourable/illegal institutions or to others connected with the scheme. Online scam can occur in chat rooms, email, SMS or on websites.

SOCIAL ENGINEERING

Social engineering is the art of manipulating people into revealing confidential or personal information. It is typically trickery for the purpose of information gathering, fraud, or access to computer systems.

PHISHING

Phishing is a technique of dishonestly obtaining private information. Typically, the phisher sends an e-mail or SMS that appears to come from a legitimate business – e.g. a bank, or credit card company requesting "verification" of information and threatens if it is not provided. The e-mail usually contains a link to a fake web page that seems legitimate, with company logos and content and has a form requesting your personal information.

CHILD GROOMING

Child grooming is when an adult becomes friends with a child in order to earn their trust, in preparation for sexual activity with the child, or exploitation. Child grooming may be used to attract minors to criminal activity such as child prostitution or child pornography.

CHILD PORNOGRAPHY

Child pornography refers to images or films (also known as child abuse images) portraying sexually explicit activities involving a child. In Brunei Darussalam it is a crime to produce, distribute, receive, or possess child pornography.

INTERNET SAFETY TIPS

As a parent, it is important for you to educate yourself on the latest online threats, establish rules and discuss safety practices in order to educate your kids about safe Internet use. Teenagers are particularly at risk because they mostly get online unsupervised and are more likely than younger kids to participate in online activities.

Here are some tips to help you protect your kids when they are on the Internet:

1 ESTABLISH GENERAL RULES

Set reasonable rules and guidelines for computer use for your kids, discuss the rules and post them near the computer to remind them.

- Encourage your kids to share their Internet experience with you.
- If they visit chat rooms, use instant messaging, play online games or other activities that require a login name to identify themselves, help them to choose a name that doesn't reveal any personal information about themselves.
- Tell your kids not to give out any identifiable information such as their name, home address, telephone number, school name or even detailed information of their whereabouts.
- Tell your kids that not everything they read or see online is true. Encourage them to ask you if they're not sure.
- Make sure your kids know never to meet anyone they met online face-to-face without talking with you about the situation.
- Teach your kids good ethics while on the Internet and always be polite.

2 DECIDE WHERE YOUR KIDS CAN OR CAN'T GO ON THE INTERNET

- Create different computer accounts for your kids and password protect it.
- Control your kids' online activities by using parental control software to filter out inappropriate content, monitor the sites they visit and try to find out what they do.
- Limit their "screen time" on the Internet. For e.g. Windows 7 operating system offers parental control capability to restrict your kids' computer usage.

3 INCREASE YOUR SECURITY AND PRIVACY

- Educate yourself on current online threats to kids, such as cyber-bullying, sexting, child pornography, online scam, etc.
- Minimize your kids' exposure on the Internet by educating them about online predators and imposters.
- Block inappropriate content before your kid accidently sees it by using parental control software.
- Use Anti-Virus and Anti-Spyware programs to help detect harmful viruses, worms, Trojan horse and any other unwanted software.
- Adjust Internet browser settings to help you control your browser security and privacy.

4 STAY INVOLVED WITH YOUR KIDS' ONLINE ACTIVITIES

- Monitor your kids' activities on the Internet; always check who they are chatting with, what types of games they play, etc.
- Learn their Internet habits and monitor what they like to do online.
- Occasionally spend time with your kids while they are on the Internet and guide them when they need help.

5 TEACH YOUR KIDS ABOUT SOCIAL NETWORKING SAFETY

These days, kids actively use social networks to connect with friends from school, family, or other people around the world. They may use social networking sites designed for adults such as Windows Messenger, YouTube, MySpace, Flickr, Twitter, Facebook and others. Parents should help their kids understand that social networking sites can be viewed by anyone with Internet access, thus the information they publish can make them exposed to scams, phishing, cyber-bullying and Internet predators.

Here are some tips that parents can teach their kids to use social networking safely:

- Tell your kids never to post any photographs without your permission and never reveal too many details in pictures.
- Tell your kids they should never meet online friends in person. Explain to them that online friends may not always be who they say they are.
- Communicate with your kids about their experience. Advise them to inform you if anything they see on the Internet makes them feel uncomfortable, anxious or threatened.
- Warn your kids about expressing their emotions to strangers. Educate your kids that online predators often search out emotionally defenceless kids.
- Warn your kids about cyber bullying. Tell them that if they think they're being cyber bullied, they should share this information with you or a teacher.

6 TEACH YOUR KIDS ABOUT BLOGGING SAFETY

The popularity of blogging has increased in recent years; however the number of kids using social networking has now exceeded blogging. If your kids happen to blog about themselves, educate them on the risks of sharing detailed personal information.

Here are some tips that will help you minimize those risks:

- Establish rules for your kids' online use.
- Assist your kids in planning what to write on their blog.
- Pay attention to what your kids write and try to check out other blogs to find positive examples.
- Save the web address of your kid's blog and visit it frequently.

WARNING SIGNS:
IS YOUR CHILD AT RISK ONLINE?

Here are some signs that your kid might be at risk:

1 YOUR CHILD SPENDS TOO MUCH TIME ONLINE, ESPECIALLY LATE AT NIGHT

Your kid may be fond of staying online late at night because there is no one around who can monitor what they are doing on the Internet. Instead of hanging out with friends, they would rather spend their time chatting with strangers using social networking sites, chat rooms, instant messaging and forums. When a child spends too much time online, they become more exposed to online predators and paedophiles.

2 YOU FIND SEXUALLY EXPLICIT MATERIAL IN YOUR CHILD'S COMPUTER

It is unusual for kids to be interested in that type of material at a young age. So if you find some on your kid's computer, it could mean that they are visiting sites that they shouldn't be looking at, or someone is providing them with it. Online predators use pornographic material in order to start sexual discussions and seduction.

3 YOUR CHILD RECEIVES PHONE CALLS OR TEXTS FROM SOMEONE YOU DON'T KNOW

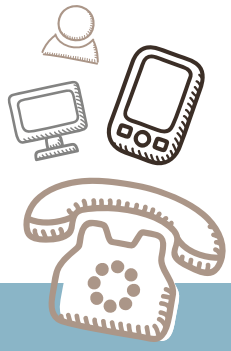
Most online predators will eventually want to talk to their potential victim on the phone, and often make arrangements to meet in person. Keep an eye on your kid's behaviour while on the phone – if they seem anxious or nervous while whispering on the phone, there might be something suspicious going on.

4 YOUR CHILD RECEIVES GIFTS FROM SOMEONE YOU DON'T KNOW

Online predators often send letters, photos and gifts while building a relationship with their potential victims.

5 YOUR CHILD BECOMES QUIET AND DISTANT FROM FAMILY AND FRIENDS

Kids who are lonely or emotionally detached from their family are likely to spend most of their time online in search for love, care and attention. Online predators will take advantage and make the kid feel like they care, while their family does not. This creates further tension with their family. Alternatively, kids may also become withdrawn after sexual victimization.



USEFUL CONTACTS & LINKS

993 ROYAL BRUNEI POLICE FORCE

141 COMMUNITY DEVELOPMENT DEPARTMENT, MINISTRY OF CULTURE, YOUTH & SPORTS

SECURE VERIFY CONNECT

www.secureverifyconnect.info

FOR MORE INFORMATION

Get Net Wise
www.getnetwise.org

I Keep Safe
www.ikeepsafe.org

i-Safe Inc.
www.isafe.org

OnGuard Online
www.onguardonline.gov

Stay Safe
www.staysafe.ie

WiredSafety.org
www.wiredsafety.org

STOP Cyberbullying
www.stopcyberbullying.org

Stay Safe Online
www.staysafeonline.org

Stop Bullying
www.stopbullying.gov

Cybersmart
www.cybersmart.gov.au

PARENTAL CONTROL SOFTWARE

Keylogger for MacOSX
www.keylogger-mac.com

PC Tattletale
www.pctattletale.com

Sniper Spy
www.sniperspy.com

USB Keylogger
www.usbkeyloggers.com

SEARCH ENGINES FOR KIDS

Ask Kids
www.askkids.com

Quintura for Kids
www.quinturakids.com

KidRex
www.kidrex.org

By reading this handbook,

you have taken the first step to helping your child have an enjoyable and safe Internet experience. It's now time to take action by exercising the main tips discussed earlier.

As a parent, you have a responsibility to keep your child safe, offline as well as online. If you think your child is in serious risk from an online predator, you should contact the relevant agency to lodge a report.