CARIBBEAN CYBER SECURITY CENTER

Caribbean Cyber Security Center – *"The Good Guys"*

www.caribbeancsc.com

CARIBBEAN CYBER SECURITY CENTER

“Caribbean Cyber Security & Scams”

THE TIME FOR AWARENESS AND VIGILANCE IS NOW

Caribbean Cyber Scams & Security – About Us

CARIBBEAN CYBER SECURITY CENTER

- ICT Governance Support
- Information Security Program Development & Support
- Vulnerability Assessment
- Penetration Testing
- Security Operational Assessment
- Incident Response
- Computer Security Incident Response Team (CSIRT) Support
- Cyber Security Awareness Training (THINKCLICKSURF)

Caribbean Cyber Scams & Security – Our Current Posture

CARIBBEAN CYBER SECURITY CENTER

- A Caribbean Cultural and Mental shift to exercise vigilance with respect to cyber scams and overall cyber security is essential.
- We must establish a Caribbean Centric Framework for cross border collaboration to fight Cyber Crime. (CARICERT)
- We must address false pride as it pertains to network security.
- We must navigate bureaucratic roadblocks and strengthen cyber crime laws and legislation regionally.
- We must actively defend our personal and professional cyber borders (work, home, school, mobile, physical)
- We must raise the overall level of “Cyber Security Awareness” regionally

Caribbean Cyber Scams & Security – “The Players & Weapons”

CARIBBEAN CYBER SECURITY CENTER

The Players

- International Crime Organizations
- Traditional Organized Crime
- Professional Hackers
- Hacktivist
- Spammers
- Insider Threat

The Weapons

- Botnets
- Phishing
- Ransomware
- SQL injections
- Targeted Viruses
- Internet Attack tools (Metasploit)
- Credit Card Fraud Devices
- Physical Devices (Key Loggers)

“Cyberattack incidents increased anywhere from **8 to 40%** *last year in Latin America and the Caribbean, depending on the country -- and that's only among nations that reported or knew about the threats hitting them, according to a new report published today by Trend Micro in collaboration with the Organization of American States (OAS).”*

Caribbean Cyber Scams & Security – “Black Market Demand”

CARIBBEAN CYBER SECURITY CENTER

- Exploit code for known flaw - $100-$500 if no exploit code exists
  - Price drops to $0 after exploit code is “public”
- Exploit code for unknown flaw - $1000-$5000
  - Buyers include iDefense, Russian Mafia, China etc
- List of 5000 IP addresses of computers infected with spyware/trojan for remote control - $150-$500
- List of 1000 working credit card numbers - $500-$5000
  - Price has increased since Operation Firewall
- Annual salary of a top-end skilled black hat hacker working for spammers - $100K-$200K

CARIBBEAN CYBER SECURITY CENTER

SHOCKING SCALE: NUMBER OF VICTIMS

1 MILLION+ VICTIMS A DAY

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES

50,000 VICTIMS EVERY HOUR

820 VICTIMS EVERY MINUTE

14 VICTIMS EVERY SECOND

CARIBBEAN CYBER SECURITY CENTER

4X MORE PHISHING ATTACKS IN 2013 COMPARED TO THE 2012 REPORT

95% OF ESPIONAGE ATTACKS INVOLVE PHISHING

47% OF MALWARE VECTORS INVOLVE ATTACHMENTS

LIKELIHOOD OF GETTING AT LEAST 1 TARGET TO CLICK ON A PHISH IF YOU RUN A CAMPAIGN TWICE

29% OF BREACHES USED SOCIAL ENGINEERING

OF THOSE BREACHES PHISHING WAS USED AS THE ATTACK VECTOR:

Profile of a HACKED system

CARIBBEAN CYBER SECURITY CENTER

"WHAT HACKERS CAN DO WITH A HACKED SYSTEM"

- Phising Site
- Malware Download Site
- Piracy Server
- Child Porn Server
- Span Server

- Webmail Spam
- Stranded Abroad Advance Scams
- Harvesting Email Scams
- Access to Corporate Email

- Online Gaming
- Online Gaming Goods\Currency
- PC Game License Keys
- Operating Systems License Key

- Facebook
- Twitter
- LinkedIn
- Google

- Spam Zombie
- DDos Extortion Zombie
- Click Fraud Zombie
- Anonymization Proxy
- CAPTCHE Solving Zombie

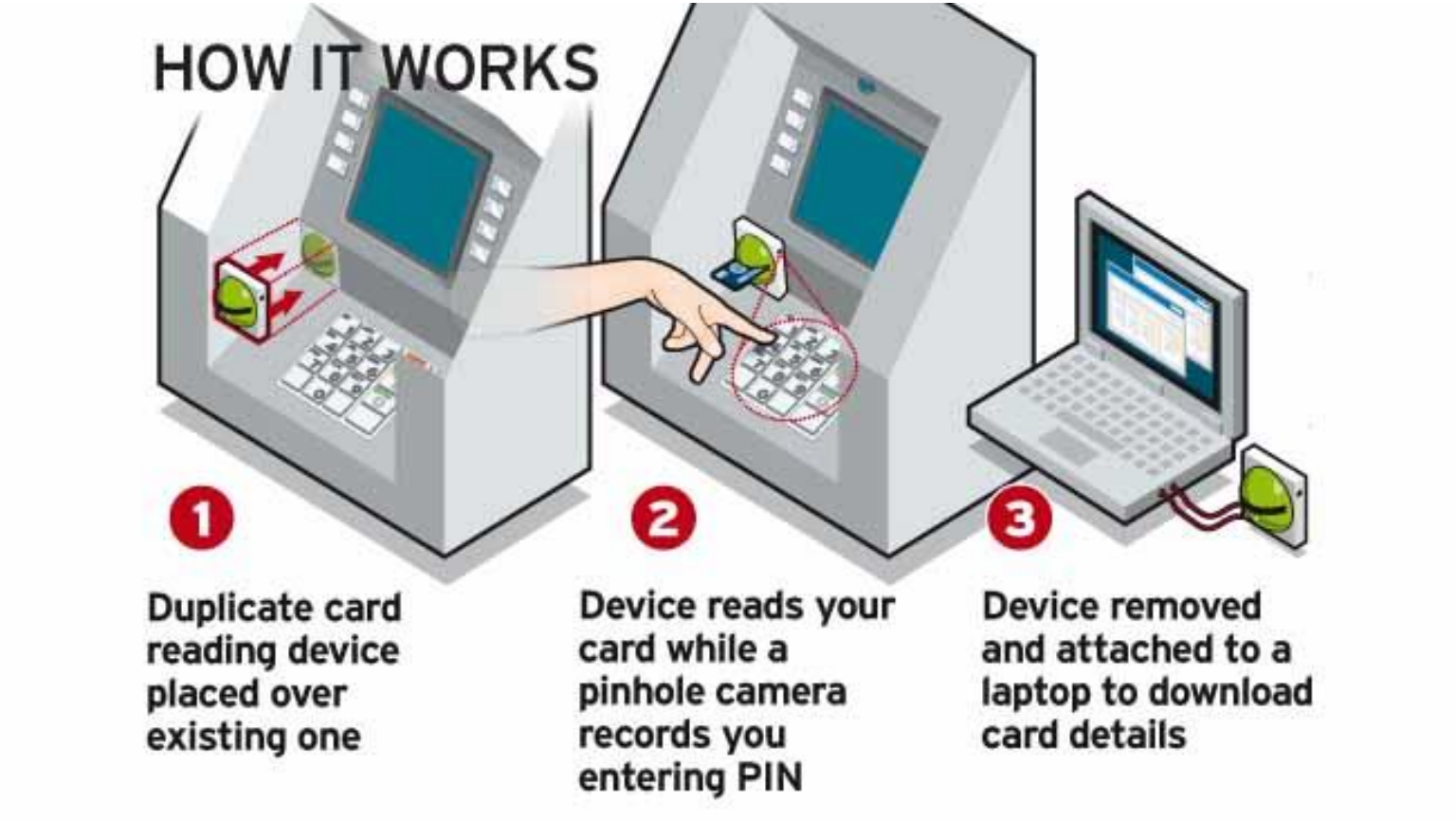
- eBay/Paypal Fake Auctions
- Online Gaming Credentails
- Web Site FTP Credentials
- Skpe/Voip Credentials
- Client Side Encryption Certificates

- Bank Account Data
- Credit Card Data
- Stock Trading Account
- Mutual Fund/401K Account

- Fake Antivirus software
- Ransomware
- Email Account Ransom
- Webcam Image Extortion

Caribbean Cyber Scams & Security – “Skimming Device” (Example)

CARIBBEAN CYBER SECURITY CENTER



Avoiding Traps

Security experts and law-enforcement officials offer this advice on protecting your personal information from criminals.

- Don't respond to phone or email messages that are unsolicited or from unknown senders. Likewise, don't open or forward attachments from unknown sources.
- If a message appears to be from a financial institution, contact your financial institution directly using a phone number you obtain independently from a bank statement or phone book.
- Install firewalls and up-to-date antivirus software. Also install updates, when available, to your computer's operating system, Web browsers and third-party applications, such as RealPlayer.
- Check that a Web site connection is secure before sending information to financial institutions or retailers. Check the browser for an "s" in the prefix before a Web address so that it reads "https." Look for the padlock icon, which many browsers display to indicate encryption is in place so that information you send is less likely to be intercepted in transit.
- If you believe your computer is compromised, reset your password immediately. Change user names and passwords for any sensitive Web sites that are visited on that computer, such as banking and credit cards sites.

Top Cyber Security Trends and Threats

CARIBBEAN CYBER SECURITY CENTER

Trend\Threat	Brief Description
Mobile Device Breaches	As the use of mobile devices grew in 2013, so too has the volume of attacks targeting them. Each mobile device provides an avenue of opportunity for potential cyber attacks.
Ransomware	Ransomware is a type of malware that is used for extortion. The attacker distributes malware that takes over a system.
Social Media	Attackers are increasingly looking to exploit these sites and the variety of Personally Identifiable Information PII being shared.
Hactivism	Attacks carried out as cyber protests for politically or socially motivated purposes have increased, and are expected to continue in 2013. Common strategies used by hactivist groups include denial of service attacks and web-based attacks, such as SQL Injections.
Advanced Persistent Threats	Advanced Persistent Threat(APT) refers to a long-term pattern of targeted hacking attacks using subversive and stealthy means to gain continual, persistent exfiltration of data. The entry point for these types of espionage activities is often weak perimeter security.
Spear Phishing Attacks	Spear phishing is a deceptive communication, often in the form of e-mail, text or tweet, targeting a specific individual, seeking to obtain unauthorized access to personal or sensitive data

U.S FBI Director

There are only (4) Types of Companies:

(1) Those that have not been hacked and have an opportunity to protect themselves

(2) Those that have been hacked and have done nothing to implement effective **technical**, **management** and **operations** security controls (360 view).

(3) Those have been hacked and "will" be hacked again

(4) Those that have been hacked and don't even know it (Advance Persistent Threats)

"The Time for ACTION is NOW"

HD\SW Inventory Management - Patch Management
Vulnerability Assessment – Penetration Testing
Continuous Monitoring

Layered View of Cyber Threats and Concerns

CARIBBEAN CYBER SECURITY CENTER

International Level

- Cyber Crime & Terrorism
- Unhindered growth of Botnets
- Absence of International mechanism to facilitate effective information sharing.
- Deliberate Attacks in Critical Infrastructures

National Level

- Cyber Crime & Terrorism
- Web Defacement
- Website Intrusion & Malware Propagation
- Scanning & Probing Government Networks for Weaknesses.
- Supply Chain Redirects Attacks
- Denial of Services Attacks

Organizational Level

- Domain Stalking
- Malicious Code
- Targeted Attacks
- Phishing
- Data Theft
- Insider Threat
- Financial Frauds

Individual Level

- Social Engineering
- Email Hacking & Misuse
- Identity Theft & Phishing
- Financial Scams
- Abuse Through Email
- Mobile Device Theft
- Laptop Theft

Events Across Our Region

"Just a Few"

Barbados Government Network Hacked **(March 2013)**

The Parliamentary website of the government of Trinidad and Tobago was breached by a hacker. **(April 2012)**

LIME Barbados' broadband network came under a DOS attack. **(April 2012)**

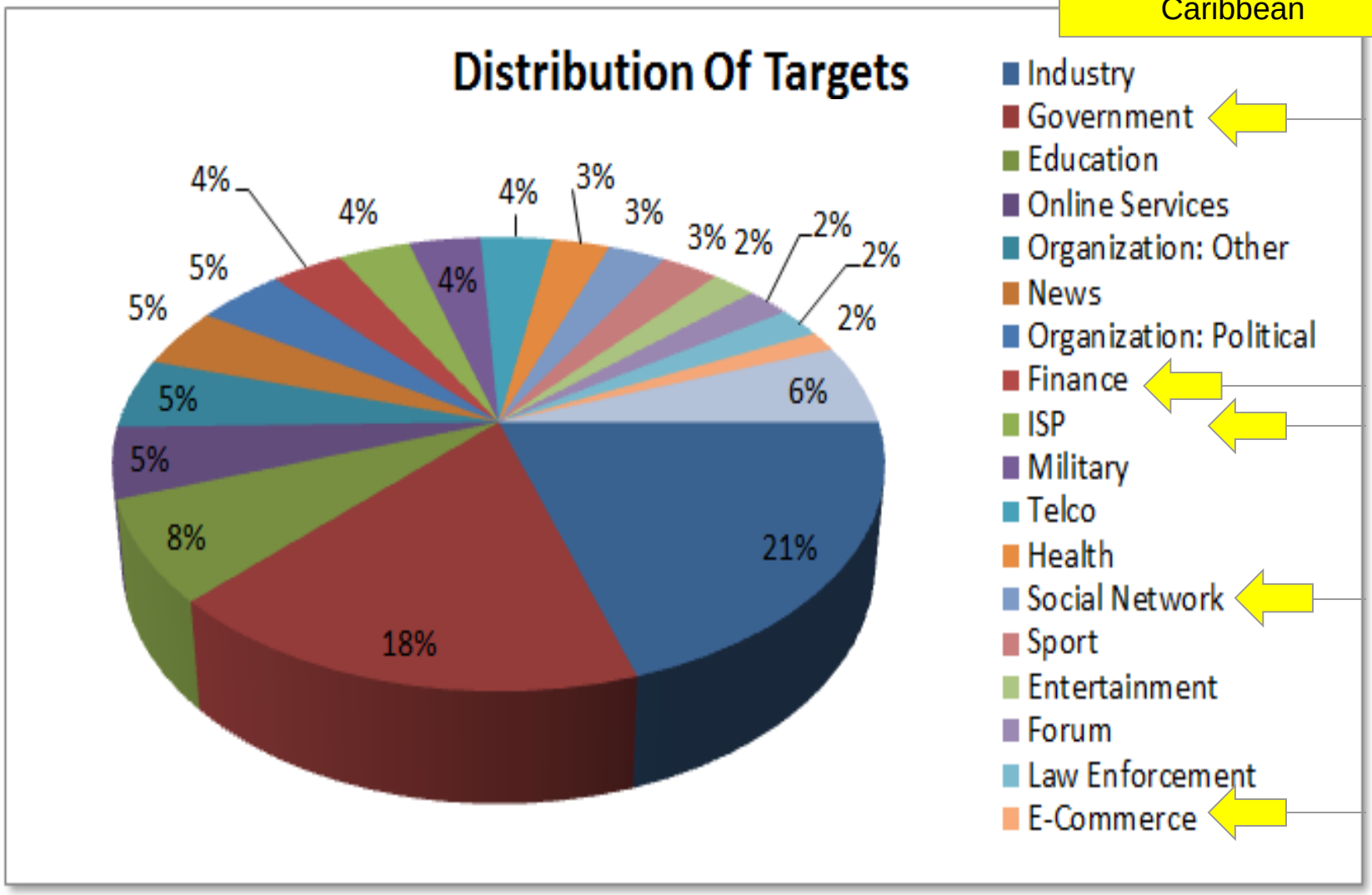
El Salvador government sites attacked. **(June 2011)**

WHO'S NEXT?

The Evolving Cyber Threat and Our Current Posture

- Lack of corporate leadership, understanding and budgetary support to proactively address the issues.
- Spike in the number of successful hackings of key public and private sector networks across the region.
- The Caribbean is one of the world's fastest growing regions for Internet usage.
- The prospect of financial gain due to regional weaknesses is drawing organized cyber criminals into the region.
- Significant lag in regional Cyber Laws & Legislation with drive security effective ICT policies, plans and procedures .
- Many Caribbean nations and organizations are still not conducting effective security awareness efforts.
- Implementation of CSIRT lagging across the region
- Lots of "TALK" little or no real "ACTION", region still trying to solve with just a technology approach.

Caribbean


Distribution Of Targets
21%
18%
8%
5%
5%
5%
4%
4%
4%
4%
3%
3%
3%
2%
2%
2%
6%
Industry
Government
Education
Online Services
Organization: Other
News
Organization: Political
Finance
ISP
Military
Telco
Health
Social Network
Sport
Entertainment
Forum
Law Enforcement
E-Commerce

Why We are Vulnerable in the Region

CARIBBEAN CYBER SECURITY CENTER

- Low level of overall Cyber Security Awareness (Public & Commercial)
- Lack of adherence to ICT, Information Assurance an Cyber Security best practices and standards (SOX, GLBA, NIST, PCI)
- Significant lag in the establishment of ICT legislation and policies across region
- Inability to effectively maintain the confidentiality, integrity and availability of systems (Management, Technical, Operational considerations)
- Shrinking budgets in challenging economic times (Return on Investment Unclear).
- Organizational difficulty obtaining management buy-in
- No sense of urgency cause nothing catastrophic has happened “yet”
- Overdependence on in-house ICT staff with no “independent” assessments being conducted (as an international best practice).

- Rapid growth in attack techniques and tools which little formal ICT knowledge to use successfully.
- Cybercrime has become the primary motivation behind cyber attacks.
- Loses in Caribbean investor confidence in the banking, finance and tourism sectors can have a major adverse reputation effect.
- Cyber Security Awareness across the region is lacking both at home and in the workplace.
- Limited regional home grown Cyber Security & Information assurance expertise.

CARIBBEAN CYBER SECURITY CENTER

Cyber Security Recommended Roadmap for the Caribbean (Public & Private Sectors)

Step	Action
A	**A**ssess your Assets, Risks, Resources
B	**B**uild Your Policy Framework(Leveraging International Best Practices)
C	**C**hoose your Controls (Technical, Management, Operational)
D	**D**eploy and Validate Your Security Controls
E	**E**ducate All Employees & Management “Annual Cyber Security Awareness Training”
F	**F**urther Assess, Audit and Test (independent assessment is KEY)

- **Loss of Investor & Visitor Confidence**
- **Inability to attract New Investors & Visitors**
- **Loss in Revenue, Customers and Productivity**
- **Losses of Confidential Data**
- **Negative Reputation - Non-Compliance with Standards**
- **Increase in Operational Costs**
- **Unplanned / Unbudgeted System Outage\Recovery**
- **Wide Reaching Stress / Uncertainty / Job losses**

Caribbean Cyber Security: ***“The Time for ACTION is NOW”***

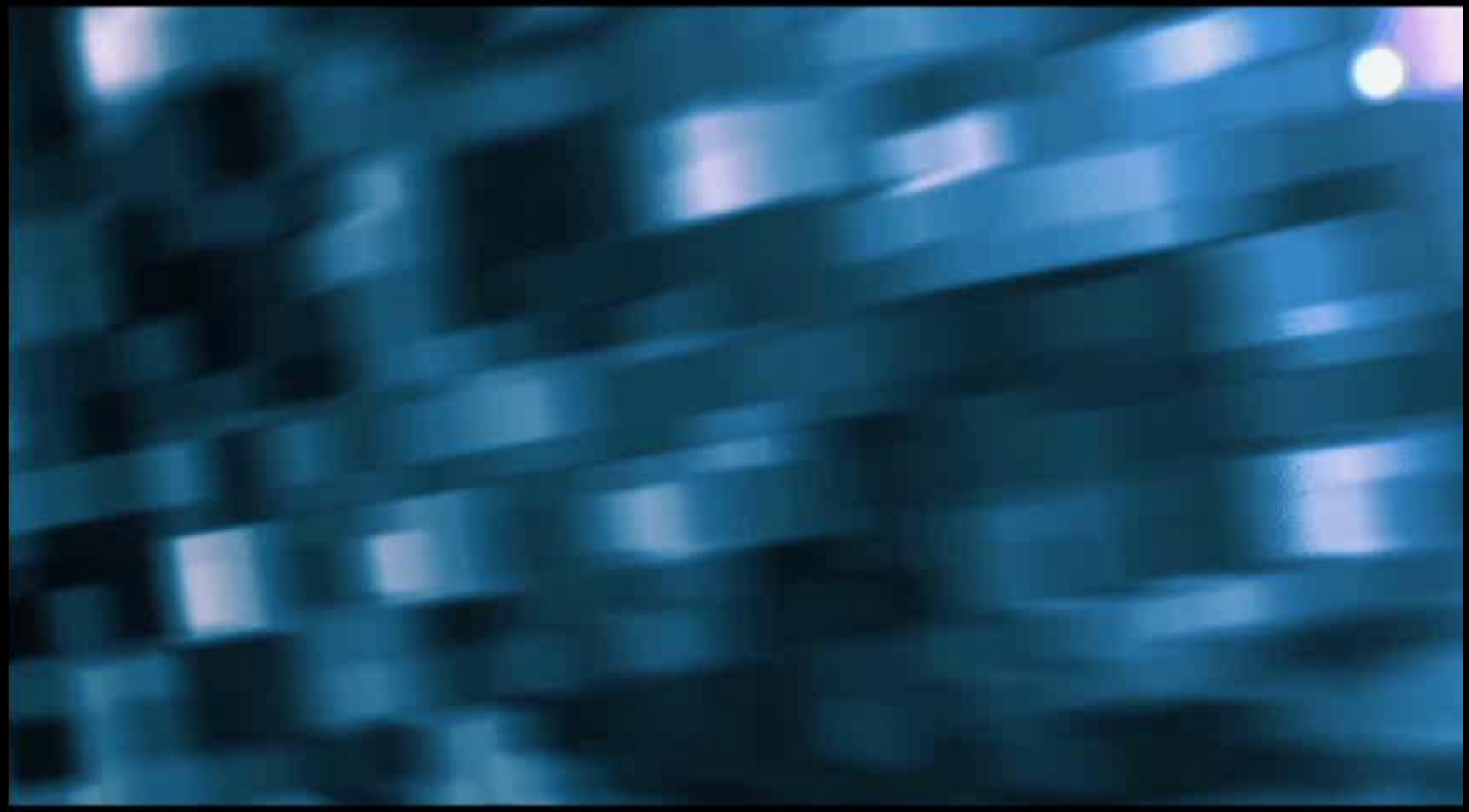
CARIBBEAN CYBER SECURITY CENTER

OCTOBER

CYBER SECURITY AWARENESS MONTH

2013

"PEOPLE, PROCESSES & TECHNOLOGY"



Official Launch of the
Jamaica Cyber Security
Awareness Program
(THINKCLICKSURF)
for Kids

http://www.thinkclicksurf.com

THINK, CLICK, SURF

www.thinkclicksurf.com/#!home/mainPage

TH!NK | CL!CK | SURF!

"Keeping Caribbean Kids Safe Online"

HOME | TIPS FOR KIDS | TIPS FOR PARENTS | PARENTS & TEACHERS | OUR REGIONAL PROGRAM | CONTACT US

select language:

English

Dutch

Papiamentu

TH!NK | CL!CK | SURF!

KEEPING CARIBBEAN KIDS SAFE ONLINE

Never buy anything over the Internet without your parent or guardian's approval.

Request a school visit

2:32 PM
9/11/2013