NC State Office of the Controller
05/20/20 Webinar

Resources and Additional information

NC DPS Emergerncy Management Cyber Unit
North Carolina's Fusion Center (NC ISAAC)

NC Department of Information Technology

How To Report

Major Ongoing Incident – Network Disabled

North Carolina Emergency Management

24 Hour Operations Center

919-733-3300 or 1-800-858-0368

Incidents Identified and Addressed/Addressing

North Carolina Dept. of Information Technology

https://it.nc.gov

"Statewide Cybersecurity Incident Report Form"

Citizen & Small Business

www.fraudsupport.org

Crimes

FBI / Local Police

Tips from the FBI

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.

Tips from the FBI, continued

- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.

Tips from the FBI, continued

- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).
- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

FBI – DHS CISA 05/12/20

Official website of the Department of Homeland Security

Search

Services Report

About Us Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Alerts > Top 10 Routinely Exploited Vulnerabilities

Alert (AA20-133A)

More Alerts

Top 10 Routinely Exploited Vulnerabilities

Original release date: May 12, 2020

Print Tweet Send Share

Mitigations for the Top 10 Most Exploited Vulnerabilities 2016–2019

Note: The lists of associated malware corresponding to each CVE below is not meant to be exhaustive but instead is intended to identify a malware family commonly associated with exploiting the CVE.

CVE-2017-11882

- Vulnerable Products: Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 Products

NC DIT

https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

NC IT: Cybersecurity Awareness

https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

Home | Services | Programs | Resources | About | News | Service Desk

Cybersecurity Tips

- Use up to date "anti-virus software"
- Do not open e-mail from unknown sources
- Use "hard to guess" passphrases
- Protect your computer files with a "firewall"
- Don't share your computer with strangers - "peer to peer file sharing"
- Update your computer's operating system and applications regularly
- Shut down your computer when not in use
- Use Instant Messengers/Chat wisely
- Make sure you know what to do in the event of a computer infection
- Regularly back-up your computer data
- Use encryption products to protect data
- Take advantage of security features in wireless access points

Donate to Hurricane Recovery

NC DIT

NC IT: Cybersecurity Awareness

https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

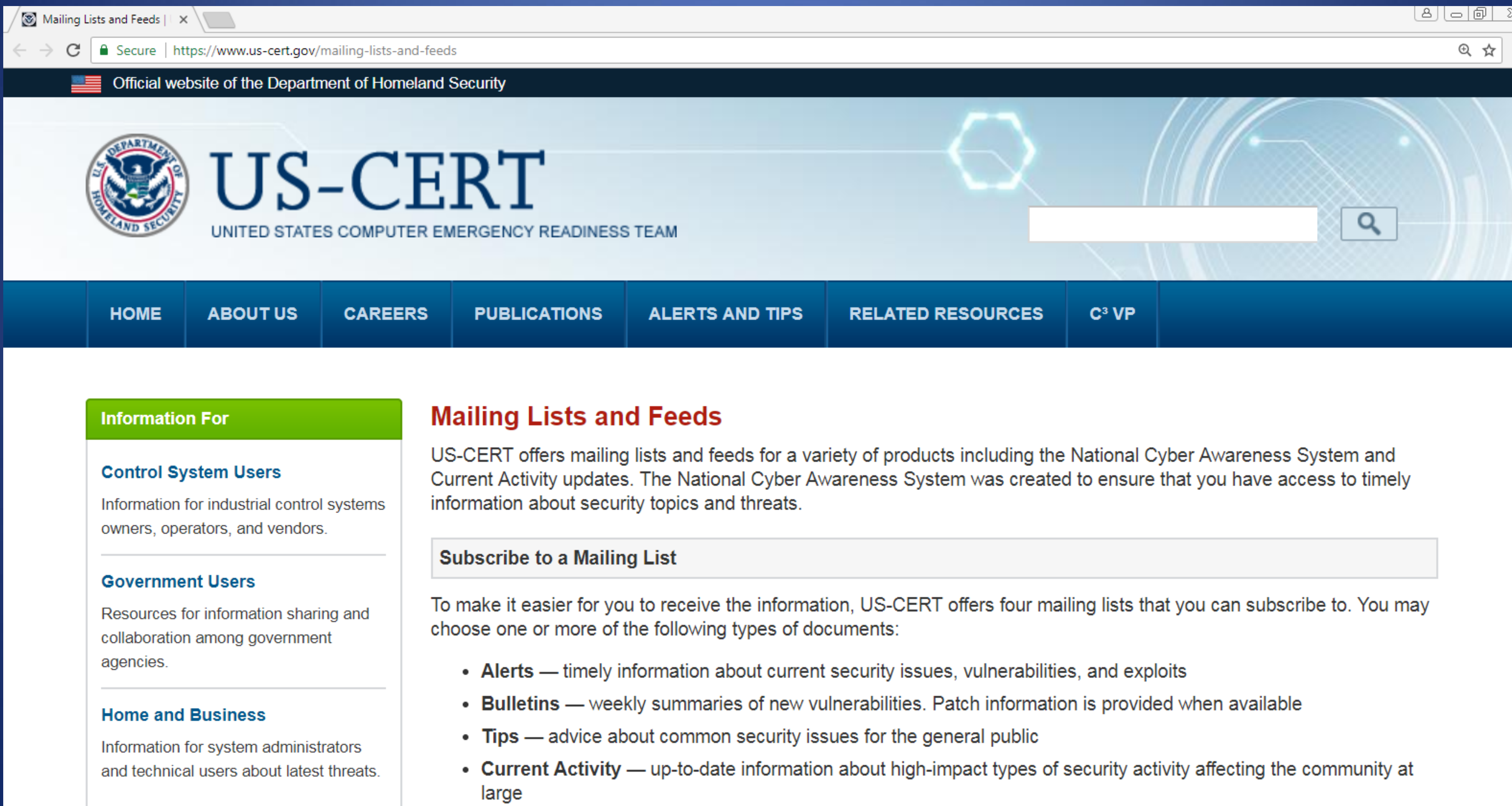
Home | Services | Programs | Resources | About | News | Service Desk

Hot Links

- Newsletters
  - Center for Internet Security Newsletters
  - SANS OUCH! Security Awareness
- State of NC Resources
  - Statewide IT Policies
  - State of NC Information Security Incident Reporting
  - NC Consumer Protection
- Center for Internet Security (CIS)
  - Cybersecurity Toolkit
  - CIS Whitepapers
  - CIS Webinars
- US-CERT
  - Safeguarding Your Data
- Governor's Proclamation for Cybersecurity Awareness Month
- 2017 Cybersecurity Awareness Symposium
  - ESRMO - 2017 Incident Training
  - McAfee – Leveraging Threat Intelligence
  - IBM – State of NC QRadar Threat Hunting Workshop
  - NCSAM "GET INVOLVED" InfoGraphic
- Cyber Crime Prevention Flyers
  - Configuring Facebook
  - Configuring Google+
  - Configuring LinkedIn
  - Configuring Twitter
  - Social Networking Safety Tips

Donate to Hurricane Recovery

Plenty of good resources



SANS

Google

SANS Ouch

All | Shopping | News | Maps | Images | More | Settings | Tools

About 442,000 results (0.34 seconds)

OUCH! Newsletter | SANS Security Awareness - SANS.org
https://www.sans.org/security-awareness-training/ouch-newsletter
OUCH! is the world's leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the **SANS** Security Awareness team, instructors and community members.

The All New OUCH!
We are super excited to announce that not only is the February ...

Securing Your Mobile Devices
Securing Your Devices. It may surprise you to know that the ...

More results from sans.org »

SANS Institute: Newsletters
https://www.sans.org/newsletters
OUCH! is the world's leading, free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the **SANS** Securing The Human team, **SANS** instructor subject matter experts and team members of the ...
Newsbites · RISK · Editorial Board · Security Awareness Newsletter

SANS Security Awareness

SANS SECURITY AWARENESS

GDPR | S

Products | Why SANS | About | Reports | Case Studies | Resources

APRIL 2018

Stop That Phish

Tonia Dudley, Director, Security Awareness
APR 2, 2018
Phishing

Translations

DOWNLOAD

MARCH 2018

Top Tips to Securely Using Social Media

Dr. Jessica Barker, Cybersecurity Consultant
MAR 5, 2018
Social Media

Translations

DOWNLOAD

FEBRUARY 2018

Securing Your Mobile Devices

In this issue of OUCH!, we walk you through some simple steps to keep you and your devices safe and secure.

FEB 5, 2018
Mobile Devices

Translations

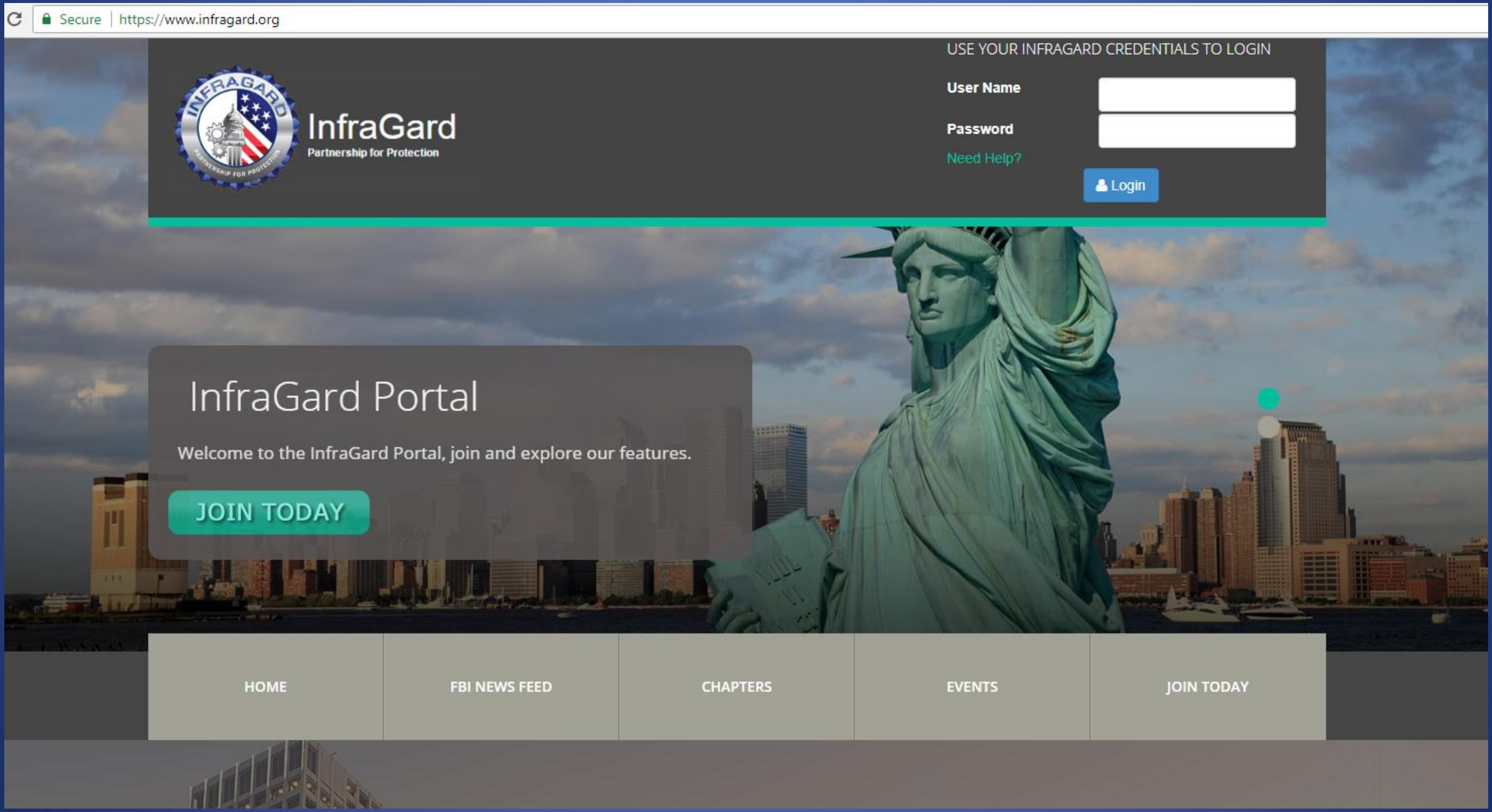
DOWNLOAD

JANUARY 2018

Creating a Cybersecure Home

In this issue of OUCH!, we walk you through critical steps to ensuring that your home is cybersecure.

www.infragard.org



Additional Information

- The following are some slides containing information and associated resourses intended to address some cyber threats individuals may be exposed to in their personal lives.

What can you do at home?

- Run <u>updated</u> anti-virus software
- Use a firewall
  - Protects against infiltration and exfiltration
- Email scanner
- Webpage/surfing protection
- The above usually come with a Security Suite which can automatically update and run.
- Update your Operating System
  - Start/Search Update/Windows Update
  - Set it to update automatically

What can you do at home?

- Use Common Sense ;-)
- Install programs from trusted sources
  - Do not use illegal file sharing programs
  - Do not travel on the dark web
- Do not click on anything unless you know what it is and where it came from
  - Find (Bank) sites on your own
  - Look at the URL
- Never send anyone your password

Online Identity Theft

- “Steal” your identifying information
  - Social security number
  - Mother’s maiden name
  - Bank account number, user id, password
  - Credit/Debit Card numbers & pin
  - Date of birth
  - Online credentials

www.consumer.gov

www.consumer.gov/jobs

How do I know a job is a scam?

Most fake job offers have things in common. A job scam:

- promises you a job
- guarantees that you will make money
- often says you can work at home
- might offer government jobs no one knows about

Scammers advertise fake jobs:

- in the newspaper
- online
- on signs, posters, and flyers

What does a fake job offer look like?

An ad for a job that would be a scam might look like this:

www.fbi.gov

Secure | https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud

SCAMS AND SAFETY

Nigerian Letter or "419" Fraud

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed, or e-mailed, from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number given in the letter or return e-mail address provided in the message. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist, and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will along with losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419 fraud."

Tips for Avoiding Nigerian Letter or "419" Fraud:

- If you receive a letter or e-mail from Nigeria asking you to send personal or banking information, do not reply in any manner. Send the letter or message to the U.S. Secret Service, your local FBI office, or the U.S. Postal Inspection Service. You can also register a complaint with the Federal Trade Commission's Complaint Assistant.
- If you know someone who is corresponding in one of these schemes, encourage that person to contact the FBI or the U.S. Secret Service as soon as possible.
- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.

www.consumer.gov

https://www.consumer.gov/articles/1019-money-wiring-scams

Managing Your Money | Credit, Loans and Debt | Scams and Identity Theft | Toolbox

Money Wiring Scams

What It Is | What To Know | What To Do

Share This Page

print

AAA text size

listen

What is wiring money?

When you wire money, you are sending cash to someone far away. This is also called a money transfer.

Many people wire money to family or friends in other cities or countries.

Wiring money is like sending cash. When you wire money, you cannot get the money back.

What are money wiring scams?

Dishonest people might convince you to wire money to them. They might say:

- you just won a prize but you have to pay fees to get the prize
- you need to pay for something you just bought online before they send it
- a friend is in trouble and needs your help
- you got a check for too much money and you need to send back the extra

These are not good reasons to wire money. You should never wire money to someone you do not know.

Read more

www.consumer.ftc.gov

FEDERAL TRADE COMMISSION

CONSUMER INFORMATION

MONEY & CREDIT

HOMES & MORTGAGES

HEALTH & FITNESS

JOBS &

Fake kidnappers cause genuine loss

October 20, 2015
by Bridget Small
Consumer Education Specialist, FTC

Phone scammers spend their days making trouble. They waste our time, tie up our phone lines and harass us with ugly language. Some do much, much worse. The FTC has heard from people who got calls from scammers saying, "I've kidnapped your relative," and naming a

THE FBI FEDERAL BUREAU OF INVESTIGATION

REPORT THREATS • A-Z INDEX

Search Site

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS & SERVICES | SCAMS & SAFETY | JOBS

Stories

Select Language

Home • News • Stories • 2014 • November • Virtual Kidnapping • Avoid Becoming a Victim of Virtual Kidnapping

Avoid Becoming a Victim of Virtual Kidnapping

11/04/14

In one example of virtual kidnapping, criminals targeted the parents of a young woman traveling in Mexico—whose phone and contact information they had stolen—and told the family they would cut off her fingers unless money was wired to them immediately. A female accomplice screamed in the background for effect. (The woman whose phone was taken was never in danger, and didn't know of the scheme until she contacted her family later.)

For criminals, the success of any type of virtual kidnapping depends on speed and fear. They know they only have a short time to exact a ransom payment before the victims and their families unravel the scam or authorities become involved.

Story Index

By Date

By Subject

- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases

- Communicate plans ahead of time
- Know some phone numbers
  - But they are in my (stolen/lost) phone
- Call

Other Scams

- Telephone calls
  - Grandparent
    - “This is your oldest granddaughter and I am in trouble and need bail money, don’t tell mom and dad…”
  - IRS
- Prey on the elderly
- And…If it seems too good to be true…

www.ic3.gov

Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Home File a Complaint Press Room About IC3 Lost Password

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint

Welcome to the IC3

Site Navigation

- Alert Archive
- FAQs
- Disclaimer
- Privacy Notice
- Internet Crime Prevention Tips

www.ic3.gov

Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Home | File a Complaint | Press Room | About IC3 | Lost Password

Internet Crime Prevention Tips

Internet crime schemes that steal millions of dollars each year from victims continue to plague the Internet through various methods. Following are preventative measures that will assist you in being informed prior to entering into transactions over the Internet:

- Auction Fraud
- Counterfeit Cashier's Check
- Credit Card Fraud
- Debt Elimination
- DHL/UPS
- Employment/Business Opportunities

Welcome to the IC3

Site Navigation

- Alert Archive
- FAQs
- Disclaimer

FBI Counterintelligence Brochures

Secure | https://www.fbi.gov/investigate/counterintelligence

> WHAT WE INVESTIGATE　　FBI　　Search FBI

Counterintelligence Brochures

- Economic Espionage: Protecting America's Trade Secrets
- Elicitation Techniques
- The Insider Threat: An Introduction to Detecting and Deterring and Insider Spy
- Intellectual Property Protection: Safeguard Your Company's Trade Secrets, Proprietary Information, and Research
- Safety and Security for the Business Professional Traveling Abroad
- Visitors: Risks and Mitigations
- Internet Social Networking Risks
- The Key to U.S. Student Safety Overseas
- Safety and Security for U.S. Students Traveling Abroad
- Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education
- Best Practices in Supply Chain Risk Management for the U.S. Government

Counterintelligence News

Featured Story

Study Abroad?

Telephone, Laptop & PDA Security

If you can do without the device, Do Not Take It!

Do not leave electronic devices unattended. Do not transport them (or anything valuable) in your checked baggage. Shield passwords from view. Avoid Wi-Fi networks if you can. In some countries they are controlled by security services; in all cases they are insecure.

Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Back-up all information you take and leave that at home. If feasible, use a different phone and a new email account while traveling.

Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Don't use thumb drives given to you – they may be compromised.

> ***During the Beijing Olympics, hotels were required to install software so law enforcement could monitor the Internet activity of hotel guests.***

Clear your browser after each use: delete history files, caches, cookies, and temporary internet files.

In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. All information you send electronically (fax, computer, telephone) can be intercepted, especially wireless communications. If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.

Beware of "phishing." Foreign security services and criminals are adept at pretending to be someone you trust in order to obtain personal or sensitive information.

If your device is stolen, report it immediately to the local US Embassy or Consulate.

Change all your passwords including your voicemail and check devices for malware when you return.

> ***Cyber criminals from numerous countries buy and sell stolen financial information including credit card data and login credentials (user names and passwords).***

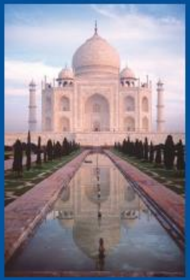
Upon Your Return

Report any unusual circumstances or noteworthy incidents to your study abroad program manager and to the FBI. Notifying the FBI will help ensure that future travel advisories take into consideration the circumstances and incidents you encountered. It is not uncommon for foreigners to contact you after your return. The FBI may be able to help you determine if these contacts pose any risk to you.

Important Numbers

Reminder

U.S. Department of Justice
Federal Bureau of Investigation



SAFETY AND SECURITY
for US Students Traveling Abroad

Living and studying in another country will be an enriching and rewarding experience, especially if you are prepared and take certain precautions. This brochure will introduce you to threats you may face and provide

Did You Know?

Groups of children and teens may swarm you and forcibly steal your personal belongings.

"Act Smart. Be Safe."

Internet Social Networking Risks

DHS.GOV

Secure | https://www.dhs.gov/stopthinkconnect

Official website of the Department of Homeland Security

Contact Us | Quick Links | Site Map | A-Z Index

Homeland Security

Topics | How Do I? | Get Involved | News | About DHS

> Get Involved > Stop.Think.Connect.

Share / Email

Stop. Think. Connect.

- Join the Campaign
- Toolkit
- Blog
- National Cyber Security Awareness Month
- Videos
- Promotional Materials
- About the Campaign
- Contact Us

Stop.Think.Connect.

National Cyber Security Awareness Month

Click here for the latest information and find out how to get involved.

The Stop.Think.Connect. Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

Cyber Tips and Resources

Safe Online Surfing (FBI)

Safe Online Surfing

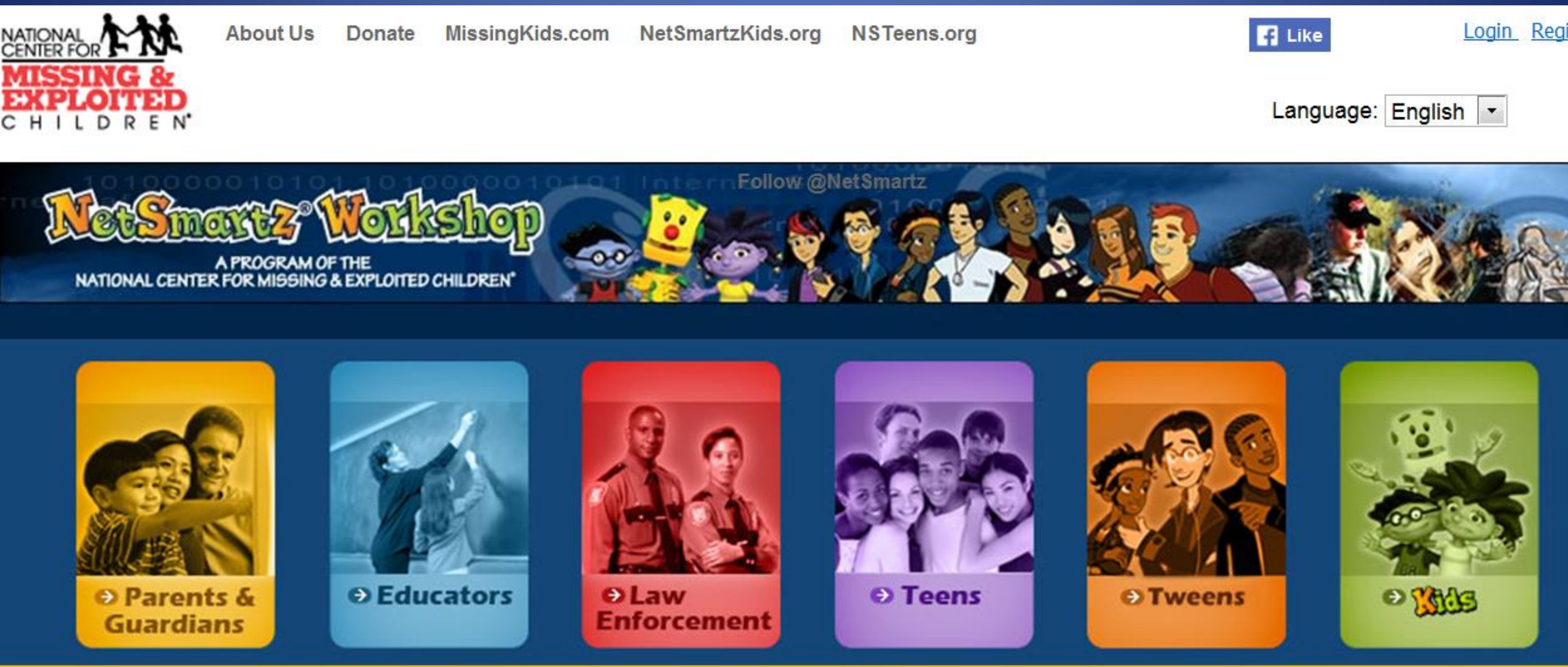
The FBI Safe Online Surfing (FBI-SOS) program is a nationwide initiative designed to educate children in grades 3 to 8 about the dangers they face on the Internet and to help prevent crimes against children.

It promotes cyber citizenship among students by engaging them in a fun, age-appropriate, competitive online program where they learn how to safely and responsibly use the Internet.

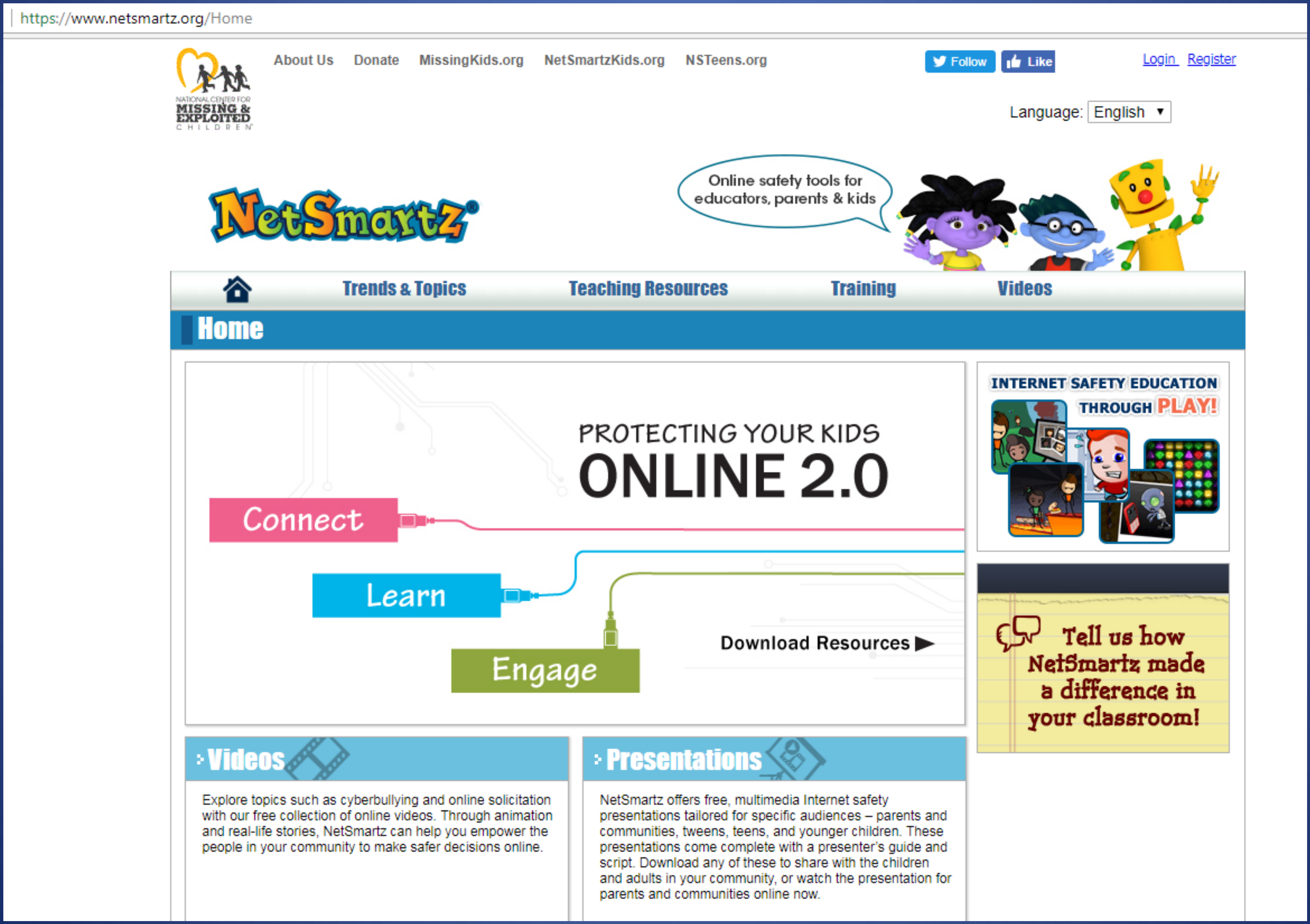
The program emphasizes the importance of cyber safety topics such as password security, smart surfing habits, and the safeguarding of personal information.

For more information, visit the Safe Online Surfing website.

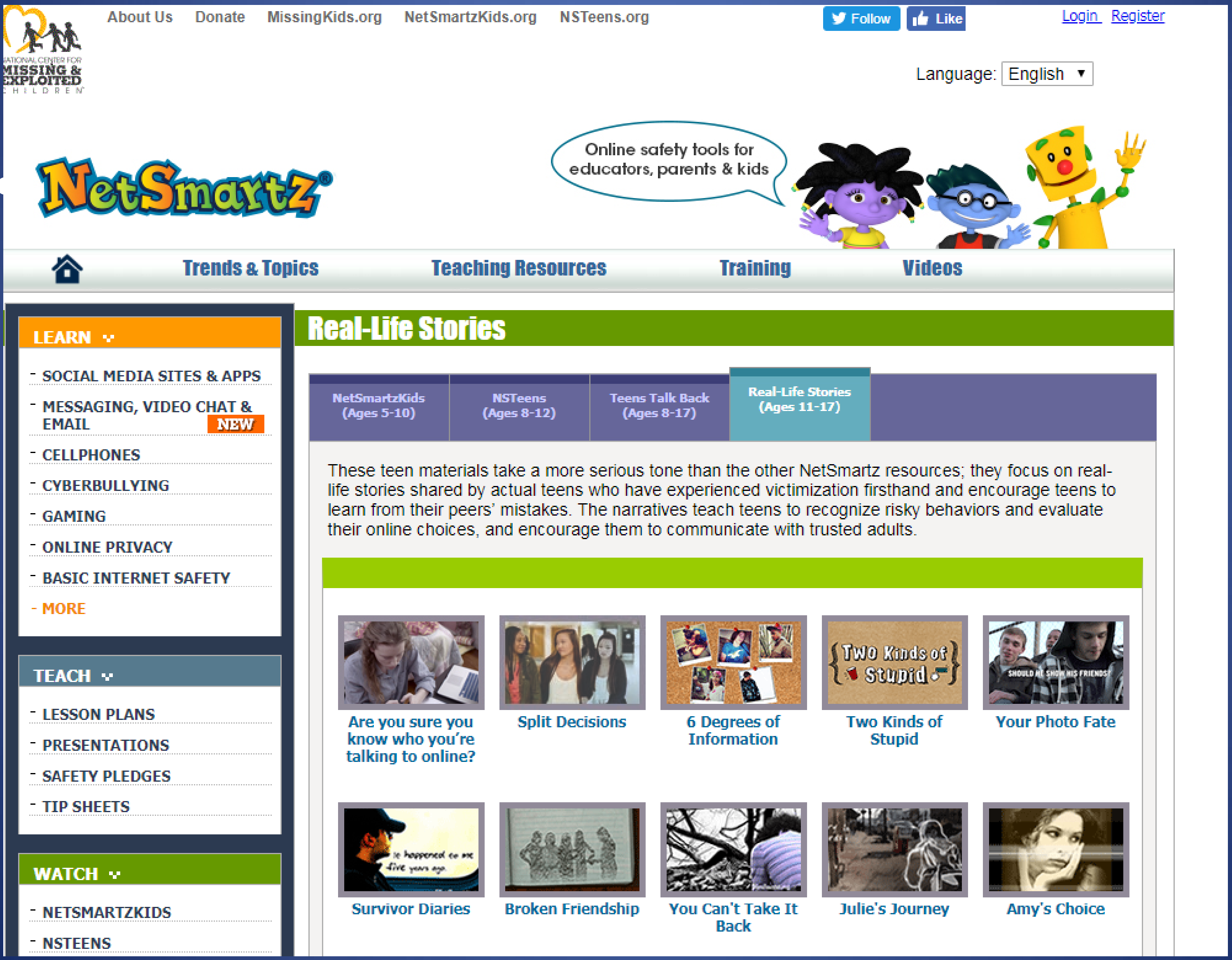
www.netsmartz.org



www.netsmartz.org



www.netsmartz.org



CYBERBULLYING

- Found Everywhere
  Phones, computers
- Public
  Visible to anyone
- Constant
  School, play, home
- Viral
  Social mediums

Final Thoughts

- There is no magic computer program to protect you, your family, or your electronics (computers & phones)!
- Use Common Sense.
- Have a family discussion.
  – Include all media: TV, Movies, Music, Video games
- This does require work on your part.
  – Congratulations on your start!
- Thank you!

Webinar Presenters

Tom McGrath

NC DPS - Division of Emergency Management

NC ISAAC Fusion Center

Mobile: 919-740-1197

Tom.McGrath@ncdps.gov / TMcGrath@ncsbi.gov

Albert Moore

NC Department of Information Technology

Enterprise Security Risk Management Office

Office: (919) 754-6245

Albert.Moore@nc.gov

INFORMATION SHARING AND ANALYSIS CENTER

ISAAC

NORTH CAROLINA

GLOBAL APPROACH TO A STATE RESPONSE