ST. JOHN LEPC

CYBER SECURITY

St. John the Baptist Parish Local Emergency Planning Committee • 2019

The Internet and Cybersecurity – YOU Can Make a Difference!

The Internet is a useful tool providing information at your fingertips for education, music, shopping and travel. Most people utilize it with good intentions. When you are on online, employ The Golden Rule and *"do unto others as you would have others do unto you."*

However, be aware of dangers and people with bad intentions who try to take advantage of others. The St. John Local Emergency Planning Committee (LEPC) wants to help you be informed and mindful so that you can continue to use the Internet safely and with confidence.

Contents

Internet Best Practices for Safety & Security

Many Internet professionals recommend that web visitors on all levels of the Internet implement the following practices:

1. Exercise Common Sense. If something seems too good to be true, it probably is. If someone is being unusually friendly, ask yourself why. Be aware of the possible consequences of a web interaction and trust your instincts.

2. Protect Your Identity. Don't use a username you've used with any website before in your email address. Never use your real name or provide personal data unless you are dealing with a trusted site that uses encryption. Do not use the same password for every online account.

3. Avoid Use of Personal Credit Cards. Rather than using a credit card that can be traced directly to you and make your financial information visible, use prepaid, single use cards for Internet purchases. If a using a credit card is necessary, be sure the website is secure by checking the web address. The address should begin with "https://," rather than "http://." The "s" on the former stands for "secure socket layer," and it means that sent and received data is encrypted.

4. Monitor Your Financial Accounts With Online Alerts. Most banks and credit card companies allow you to set up alerts anytime you receive money, make a charge, or take money from your account.

5. Do Not Download or Open Files Online, Especially From the Dark Net. If you must download something, scan it with antivirus software (or at least a free service like VirusTotal) before opening to detect viruses, worms, trojans, and other malware. Do not click on suspicious links, especially anything that advertises illegal activities.

6. Keep Your Web Browser Up-to-Date. Configure your browser for better security – the default configuration is not set up for the best security. For example, set your security level to "High" even though this disables some features such as ActiveX and Java (notable for their security breaches). Understand and modify your browser settings to your specifications for maximum protection.

Article source: https://www.moneycrashers.com/dark-web/

How to Protect Your Computer, Smart Phone and Pad

Keep Your Firewall Turned On: A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

Install or Update Your Antivirus Software: Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

Continued on page 3

National Cybersecurity Campaigns

National Cybersecurity Awareness Month (NCSAM) 2019

will promote personal accountability and encourage proactive behavior to enhance cybersecurity. Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online.

NCSAM 2019 will emphasize personal accountability and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. This year's overarching message – Own IT. Secure IT. Protect IT. – will focus on key areas including citizen privacy, consumer devices, and e-commerce security.

Article source: https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

National Cybersecurity Awareness Month – Please visit the web site at https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019 to read all the available information.

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.

Article source: https://www.dhs.gov/stopthinkconnect

37%

of teens feel overwhelmed by drama on social media.

45%

of teens associate their social media use with positive emotions such as feeling included and confident.

70%

of teens feel pressured to post content that will get a lot of likes on social media.

How to Protect Your Devices

Continued from page 2

Install or Update Your Antispyware Technology: Spyware is just what it sounds like — software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code.

Keep Your Operating System Up to Date: Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

Be Careful What You Download: Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know.

Turn Off Your Computer: With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

Article source: https://www.moneycrashers.com/dark-web/

K-8 Student Cybersecurity Tips

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 at *www.sos.fbigov.*

Article source: www.sos.fbi.gov

About NetSmartz

Since 1998, NCMEC has operated the CyberTipline, a place where the public and electronic service providers can report suspected online and offline child sexual exploitation. The millions of reports made each year uniquely situate NCMEC to identify trends and create prevention resources to address the evolving needs of kids and teens online.

NetSmartz is NCMEC's online safety education program. It provides age-appropriate videos and activities to help teach children be safer online with the goal of helping children to become more aware of potential online risks and empowering them to help prevent victimization by making safer choices on- and offline.

Article source: http://www.missingkids.org/netsmartz/home

GRADES K - 8
Simple Tips

Trust your feelings.
If something does not feel right when you are online, stop what you are doing.

Think before you click.
Don't open e-mails or download attachments from strangers.

Talk with a parent, teacher or trusted adult.
If something makes you feel uncomfortable.

Keep your personal information private.
Avoid sharing your name, address, telephone number and the name of your school when using the Internet or any apps.

Just like in real life, treat others like you want to be treated.
Do not bully or say/post anything online that could hurt other's feelings or get you in trouble.

Remember to protect your cell phone and tablet.
Use a PIN or password to lock the devices. The same tips for being safer online apply when you access the Internet from any device, such as smart phones, video game consoles, etc.

If something happens online:

- Turn off the computer monitor.
- Tell a parent, guardian, teacher or adult you trust.

Article source: www.dhs.gov/stopthinkconnect

It is important to play games that are age-appropriate. Ratings sites like ESRB.org and CommonSenseMedia.org can help you decide if a game is appropriate.

Article/tip source: http://www.missingkids.org/netsmartz/topics/gaming

9-12 Student Cybersecurity Tips

Simple Tips

1. Keep your personal information private, including the names of your family members, school, telephone number and your address.
urn off the GPS location services and your device's camera when not using them.

2. Avoid sharing your whereabouts online to avoid cyberstalking.
Wait to post event or trip photogs until you return home so criminals are not aware when you are not home.

3. Think twice before you post or say anything online; once it is in cyberspace, it is out there forever.
Remember, what you post may impact you getting or keeping a job in the future.

4. Only do and say things online that you would do or say in real life.
Think about how your decisions on what you post or say online can have positive or negative consequences later.

5. Speak up.
If you see something inappropriate, let the website know and tell an adult you trust. Do not stand for bullying – online or off.

6. Use strong passwords with eight characters or more that also use a combination of numbers, letters and symbols.
Do not share your passwords with anyone.

7. Think before you click.
Do not open e-mails from strangers and do not click on links to unfamiliar sites.

8. Be careful who you friend online and verify they are trustworthy.

9. Use privacy settings on social networking websites such as Twitter, Instagram, SnapChat and Facebook.

10. Be cautious when downloading applications on your smartphone.
They may contain malware that could infect your device.

11. Be sure to review and understand details of an app before installing.
Be wary of the information it requests.

If You've Been Compromised

Talk with a parent, guardian, teacher or adult you trust.

Keep all evidence of the interaction and write down the date and time the incident occurred.

Contact law enforcement to file a report.

If you received an online soliticitation, make a report at www.cybertipline.com or call 1-800-843-5678.

If you are the victim of online fraud, report it to the Department of Justice at www. justice.gov/criminal/cybercrime/reporting.

Article source: www.dhs.gov/stopthinkconnect

1 in 5

High School students reported being bullied at school last year

See Articles on Page 8

Internet Dangers

Dark Web

The dark web "attracts people who want to engage in things like robbery, sex trafficking, arms trafficking, terrorism and distributing child pornography." In the International Business Times, writers Charles Paladin and Jeff Stone claim electronic goods, contract killers, guns, passports, fake IDs, and hackers for hire are readily available on the dark web, in addition to illegal drugs and child pornography.

The Deep Web

The vast proportion of the web known as the deep web – sometimes called the "invisible" or "hidden" web – refers to all of the digital content that cannot be found with a search engine. It includes email in a Gmail account, online bank statements, office intranets, direct messages through Twitter, and photos uploaded to Facebook marked "private." Governments, researchers, and corporations store masses of raw data inaccessible to the general public. This content is stored on dynamic web pages (built on the fly based upon query information) and blocked, unlinked private sites. According to Trend Micro, a significant portion of the deep web is dedicated to "personal or political blogs, news sites, discussion forums, religious sites, and even radio stations."

Article source: https://www.moneycrashers.com/dark-web/

FBI

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. American companies are targeted for trade secrets and other sensitive corporate data and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators.

Article source: https://www.fbi.gov/investigate/cyber

PROTECT YOURSELF FROM ONLINE FRAUD

Stay Protected While Connected

The bottom line is that whenever you're online, you're vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

- Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection.
- Avoid free Internet access with no encryption.
- Don't reveal personally identifiable information such as your bank account number, SSN, or date of birth to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

Article source: https://niccs.us-cert.gov/sites/default/files/documents/pdf/ncsam_identitytheftandinternetscams_508.pdf?trackDocs=ncsam_identitytheftandinternetscams_508.pdf

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source.

Smart Phones

As most smartphones have GPS technology, users may unintentionally share their locations with the public. If a users' photos have GPS location-tags or if a user "checks-in" to restaurants, airports, new cities, etc., friends and followers can see exactly where that person is or has been. Each smartphone brand or model may have a different way to turn off location-tracking services. Check the settings on your child's phone, paying attention to which applications can access location data.

Article source: http://www.missingkids.org/netsmartz/topics/smartphones

Online Gaming

Online gaming has become increasingly popular with children and adults of all ages and genders in recent years. There is a vast array of game-types available online ranging from massively multiplayer online games (MMOG) to digital arcades and sports games. Gaming has been shown to have positive effects on social skills and problem solving, but it is not an activity completely without risks.

It can be hard for adults to supervise online gaming. There are thousands of online games and apps, making it hard to know exactly what children are playing. In addition, children can play from anywhere thanks to mobile gaming devices, smartphones and tablets. Games can also have confusing or inappropriate content for children. Some have adult language or are violent or sexual. Others have advertisements that let children make purchases without parental authorization.

Many online games have features that allow players to talk or IM with each other. Some of these players may:

- **Gather sensitive information like passwords and credit card numbers by scamming children or hacking directly into their accounts.**
- **Engage in the online enticement of children by having sexual conversations, request sexual images or, more rarely, ask children to meet offline. They may even try to get children to share sexual images by sharing their own images first.**

Article source: http://www.missingkids.org/netsmartz/topics/gaming

Social Media Sites and Apps

Social media sites and apps are an important part of how we all use the internet. Younger children may enjoy sites like Animal Jam that do not fit the traditional social media mold, but still allow users to communicate with each other, while older children, teens, and adults, may prefer sites like Facebook, and apps like Snapchat and Instagram.

Most social media sites and apps (including Facebook, SnapChat, Twitter, Instagram, and Musical.ly) require users to be at least 13 years old, though it is not uncommon for youths to be untruthful about their date of birth in order to gain access to the site or app. By accessing these platforms before age 13, young children are at an increased risk of encountering inappropriate content and/or contact from older users.

Article source: http://www.missingkids.org/netsmartz/topics/socialmedia

24-Hour HOTLINE
1-800-THE-LOST (1-800-843-5678)

Report It

If you think you have seen a missing child, contact the **National Center for Missing & Exploited Children** 24-hours a day, 7 days a week.

Report Child Sexual Exploitation

Use the **CyberTipline** to report child sexual exploitation. Reports may be made 24-hours a day, 7 days a week online at www.cybertipline.org.

For extensive Cybersecurity information, tools and valuable resources for students, teachers and parents, including PDF downloads, visit http://sjbparish.com/emergency_index.php

Bullying & Preventing Bullying

What Are the Consequences?

Bullying can result in physical injury, social and emotional distress, self-harm, and even death. It also increases the risk for depression, anxiety, sleep difficulties, lower academic achievement, and dropping out of school. Youth who bully others are at increased risk for substance use, academic problems, and experiencing violence later in adolescence and adulthood. Youth who bully others and are bullied themselves suffer the most serious consequences and are at greater risk for mental health and behavioral problems.

Article source: https://www.cdc.gov/violenceprevention/youthviolence/bullyingresearch/fastfact.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fviolenceprevention%2Fyouthviolence%2Fbullyingresearch%2Findex.html

If You Witness Cyberbullying:

Do not participate. Do not "like," share, or comment on information that has been posted about someone, and do not forward a hurtful text to others.

Do not retaliate or respond negatively. Angry and aggressive reactions can make a bad situation worse. Step away from the device and do not resort to blaming, shaming, or retaliation. This provides time to get calm and centered. Make it clear that others' digital behaviors are hurtful and unacceptable.

Respond privately to the person who created the hurtful message. If you feel safe doing so, it may be helpful to follow up with the person who created or shared the hurtful message privately, either online, in a phone call, or in person.

Follow up with the person who was targeted. By reaching out, you can send a powerful message that they care about the person and they do not support the negative behaviors.

Article source: https://www.stopbullying.gov/cyberbullying/establishing-rules/index.html

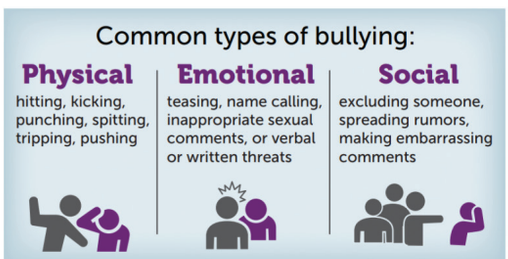
stopbullying.gov

According to StopBullying.gov, Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. It can happen via text message and within apps, on social media, forums, and gaming sites. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can also include sharing personal or private information about someone else causing embarrassment or humiliation.

Signs That A Child May Be A Victim of Cyberbullying Include:

- Avoiding the computer, cellphone, and other technological devices or appears stressed when receiving an e-mail, instant message, or text
- Withdrawing from family and friends or acting reluctant to attend school and social events
- Avoiding conversations about computer use
- Exhibiting signs of low self-esteem including depression and/or fear
- Has declining grades
- Has poor eating or sleeping habits

*Article source: http://www.missingkids.org/*netsmartz/topics/cyberbullying



DIGITAL AWARENESS
Parental Tips

The digital world is constantly evolving with new social media platforms, apps, and devices, and children and teens are often the first to use them. Some negative things that may occur include cyberbullying, sexting, posting hateful messages or content, and participating in negative group conversations. If your child posts harmful or negative content online, it may not only harm other children; it can affect their online reputation, which can have negative implications for their employment or college admission.

While you may not be able to monitor all of your child's activities, there are things you can do to prevent cyberbullying and protect your child from harmful digital behavior:

- **Monitor a teen's social media sites, apps, and browsing history, if you have concerns that cyberbullying may be occurring.**
- **Review or re-set your child's phone location and privacy settings.**
- **Follow or friend your teen on social media sites or have another trusted adult do so.**
- **Stay up-to-date on the latest apps, social media platforms, and digital slang used by children and teens.**
- **Know your child's user names and passwords for email and social media.**
- **Establish rules about appropriate digital behavior, content, and apps.**

Article Source: https://www.stopbullying.gov/cyberbullying/digital-awareness-for-parents/index.html