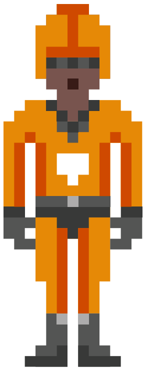


CYBERSECURITY CHAMPIONS

2022 // Kids Safe Online

ACTIVITY BOOK

CYBERSECURITY CHAMPIONS!

The U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has designated the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) as the key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

Every year, the MS-ISAC conducts a National Cybersecurity Awareness Poster Contest to encourage young people to use the internet safely. The contest is open to all K-12 students in all 50 states, the District of Columbia, U.S. territories, U.S. tribes, and U.S. military installations worldwide.

This year marks the second iteration of our cyber safety activity book. It includes cybersecurity-related puzzles, word searches, word scrambles, coloring pages, and poster contest artwork. This activity book's artwork was developed by grade K-12 students who participated in the 2021/2022 MS-ISAC National Cybersecurity Awareness Poster Contest. The 13 winning submissions illustrate the safe use of the internet and mobile devices through password protection, keeping devices and software up-to-date, protecting personal information, and other important topics.

With kids spending more time online than ever before, cybersecurity is of the utmost importance. The contest is a fun yet impactful way that our kids can educate not only their peers but also everyone else on the importance of online safety. Thanks to all the students who contributed submissions, and congratulations to our winners!

Karen Sorady
Vice President for MS-ISAC Member Engagement

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

THE WINNERS!

NATIONAL WINNER

Madelyn — 8th Grade, New York

Maylin — 12th Grade, New York

Megan — 5th Grade, New York

Leila — 3rd Grade, Virgina

Valentina — 5th Grade, New York

Eliana — 12th Grade, New York

Alisa — 7th Grade, New York

Jacob — 11th Grade, Texas

Teagan — 7th Grade, South Dakota

Layan — 6th Grade, Pennsylvania

Karlie — 7th Grade, South Dakota

Ana Alicia — 8th Grade, Texas

Atikiss — 4th Grade, Montana

NOTE

For the contestants' safety, only a limited amount of information about the winners is released.

ENTER YOUR POSTER!

The next Poster Contest will be open from Sept. 26, 2022, through Jan. 23, 2023.

Winners will be featured in the 2022/2023 MS-ISAC Kids Safe Online Activity Book — Cybersecurity Champions!

Please visit https://www.cisecurity.org/ms-isac/ms-isac-toolkit/ for more information on the 2022-2023 MS-ISAC National Cybersecurity Awareness Poster Contest guidelines.

For questions, please email us at contest@cisecurity.org.

We appreciate the continued support from our integral partners.

KNOW YOUR CYBERSECURITY TERMS!

Adware
Programs that display an advertisement on the screen. They are often installed without the user realizing.

Anti-malware/Anti-virus
Software that scans computers, laptops, and mobile phones for viruses and malware.

Application
User-facing software that runs on a personal computing device. Common examples include web browsers and computer games.

Catfishing
Luring someone into a relationship either through a chatroom or social media website using a fake identity.

Clickbait
A link that entices you to click on it. Clickbait will usually use images or phrases to draw the user's attention.

Cookie
You can't eat these, but they DO keep track of your user preferences.

Cryptography
The use of coding to secure communication between two parties.

Cyber Attack
An attempt to gain unauthorized access to a computer system for the purpose of viewing, modifying, or deleting data or extorting money (ransomware).

Cyberbully
A person who hurts someone else online on purpose.

Cybercrime
Another word for computer crime, which involves malicious actors using computing devices for illegal purposes.

Cybersecurity
The use of people, processes, and technology to defend against cyber attacks and other digital threats.

Dark Web
Part of the deep web that relies on connections made between trusted peers. It is not automatically accessible by ordinary users.

Data
Information that is stored on a device or computer.

Database
A resource that stores information, usually electronic data, in an organized way.

Data Breach
A cyber attack that results in the exposure of information.

Deep Web
Part of the World Wide Web that's not indexed or searchable by search engines like Google.

Download
Save a file from the internet to your computer.

Encryption
The process of scrambling information so that it becomes unreadable to anyone who doesn't have a secret key.

Exploit Kit
Software that uses vulnerabilities to infect computing devices with viruses, malware, and other threats.

Firewall
A program that helps to prevent threats from entering the network.

Firmware
A piece of software that's embedded in a piece of hardware.

Hacker
Someone who uses computing, networking, and/or other related skills to solve a technical problem.

Hardware
The physical components of a computer system, like the wiring, monitor, laptop, or disc drive.

HTTP
Short for "Hypertext Transfer Protocol." It's central protocol for communicating data over the internet.

HTTPS
Short for "Hypertext Transfer Protocol Secure." It's an extension of HTTP that uses encryption to secure a web connection.

Human Error
A mistake committed by a human user that weakens the security of data, systems, or the organization as a whole.

Identity Theft
A crime that involves someone obtaining personal information such as a credit card, social security number, or bank account number from someone else in order to steal money or commit other harmful acts.

Identity Fraud
The act of misusing someone's identifying account(s) or information.

Information Security
A process of protecting information against unauthorized access, disclosure, and tampering.

Internet
A giant collection of computer networks that connects people and information all over the world.

Malvertising
Short for "malicious advertising," this is when digital attacks use legitimate advertising networks to spread malware.

Malware
Short for "malicious software." Programs that damage computers, steal personal information, or expose a computer to further damage by crackers.

Glossary

Man-in-the-Middle (MitM) Attack
A cyber attack in which a malicious actor is able to eavesdrop on the communications between two parties.

MMS
Short for "multimedia messaging service," MMS enables mobile users to exchange images, videos, and other multimedia files with one another.

Multi-Factor Authentication (MFA)
A method of identity and access management that requires a user to provide multiple factors of authentication as part of the login process. Factors include something you know (e.g., PIN, password), something you have (e.g., hardware token, phone), and something you are (e.g., fingerprint, facial ID).

Netiquette
Principles of behaving ethically online.

Network
Multiple computers that are connected to one another.

Password
A string of characters that helps with authenticating a user during a login process.

Passphrase
A sequence of words or text for securing access to a trusted account.

Phishing
An attempt to trick people into visiting malicious websites and/or sharing their personal information via email.

Piracy
The illegal duplication or use of copyrighted material.

Pop-up
An unsolicited advertisement.

Privacy Settings
Configuration items in devices and on websites, including social networking sites, that allow you to control who sees information about you.

Ransomware
A type of malware that encrypts a victim's information and demands a ransom in exchange for a recovery key.

Scam
Something fraudulent that's designed to cheat a victim out of something.

Scareware
A type of threat that uses social engineering techniques to trick people into buying or downloading something useless, malicious, or revealing sensitive information.

Search Engine
A web tool that enables users to locate info on the World Wide Web, such as Google Chrome

Security Settings
Configuration items, in devices or as part of social networking sites, that allow you to protect access to your account and your information.

Smishing
A form of phishing that uses SMS as its delivery vector.

SMS
Short for "short messaging service," SMS enables mobile users to exchange text messages with one another.

Social Engineering
A type of cyber attack that manipulates human users into doing something that weakens their cybersecurity like sharing sensitive data.

Social Media
A social network that is used to share personal images and information.

Software
Programs that run on your computer.

Spam
Another term for "junk email", usually an email message sent to a large number of people without their consent that promotes a product or service.

Spyware
A type of malware designed to monitor victims without their knowledge.

Streaming
Using media without downloading it. An example is listening to music on YouTube.

Surface Web
Part of the World Wide Web that's indexed by search engines like Google and reachable by the general public.

Surfing
Browsing multiple websites on the internet, usually by moving from one website to another.

Trojan
A type of malware that impersonates a legitimate program to trick users into installing it on their devices.

Troll
Someone who posts upsetting messages or images on social media for the sole purpose of gaining an emotional reaction from the viewers.

Upload
Sending information from one computer to another.

Virus
A type of malware that self-replicates, allowing it to delete files, steal data, or take over someone else's computer remotely.

Vishing
A form of phishing that uses voice-based phone calls as its delivery vector.

Vulnerability
A flaw in a piece of hardware, a piece of software, or a security system. Attackers can exploit a vulnerability for malicious purposes.

Web Server
Programs that manage a website and send web pages to the user's browser when it is asked to do so.

Whaling
A form of phishing that specifically targets senior people in an organization, like the CEO orother executives.

World Wide Web (www or web)
A system on the internet that allows you to browse through a variety of linked resources using typed commands or clicking on links.

2022 Poster Contest National Winner

Madelyn

8th Grade • New York

Wherever you go, your digital footprint follows.
Choose your path wisely.
DEAD END
TURN BACK

Cyber Point

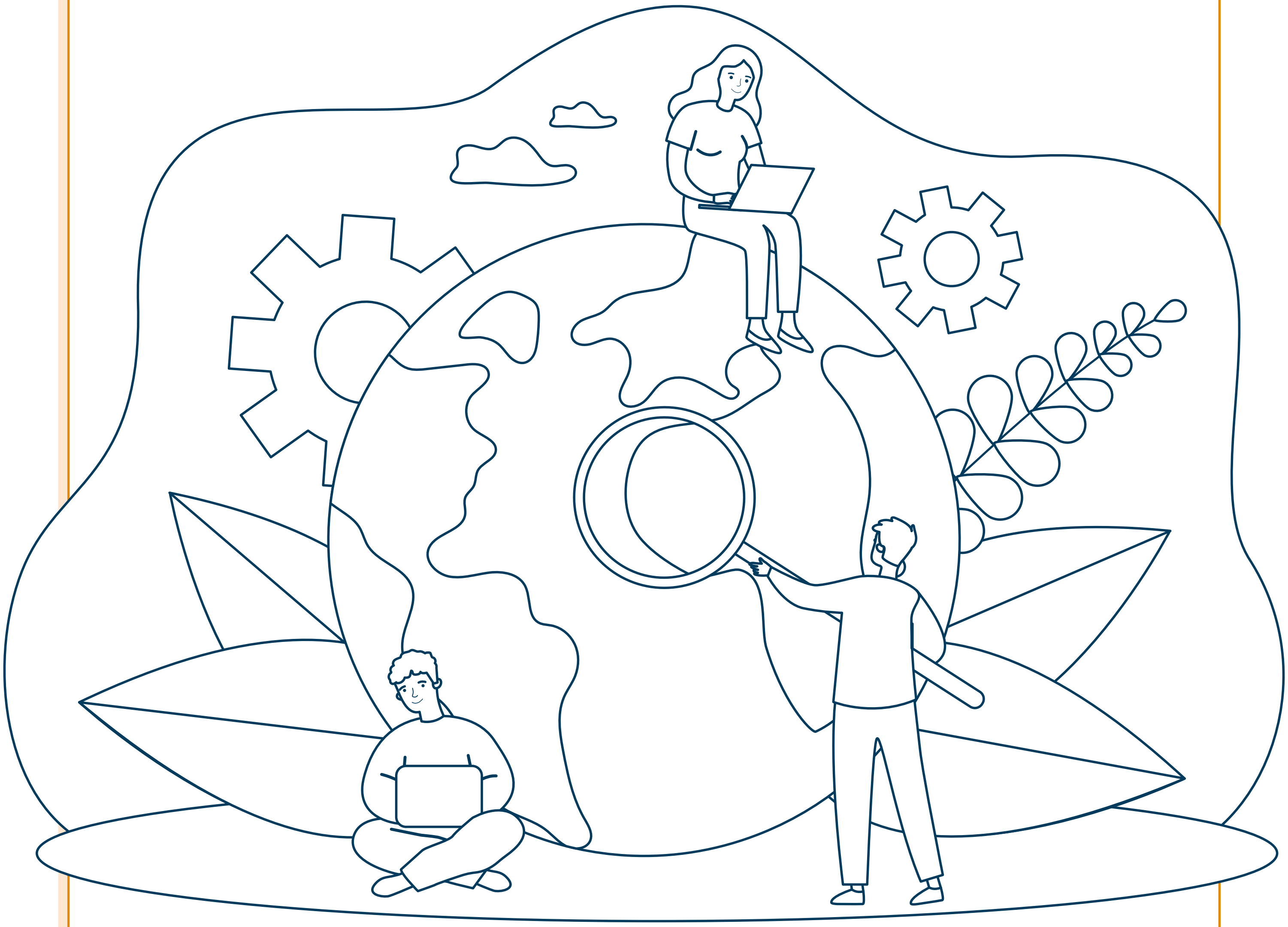
WHAT A GREAT BIG WEB!

The internet doesn't just connect laptops. It also brings smartphones, tablets, gaming systems, smart TVs, and other types of devices together under the World Wide Web. As such, each of us can do our part to secure these devices against digital attackers.

COLORING

Instructions

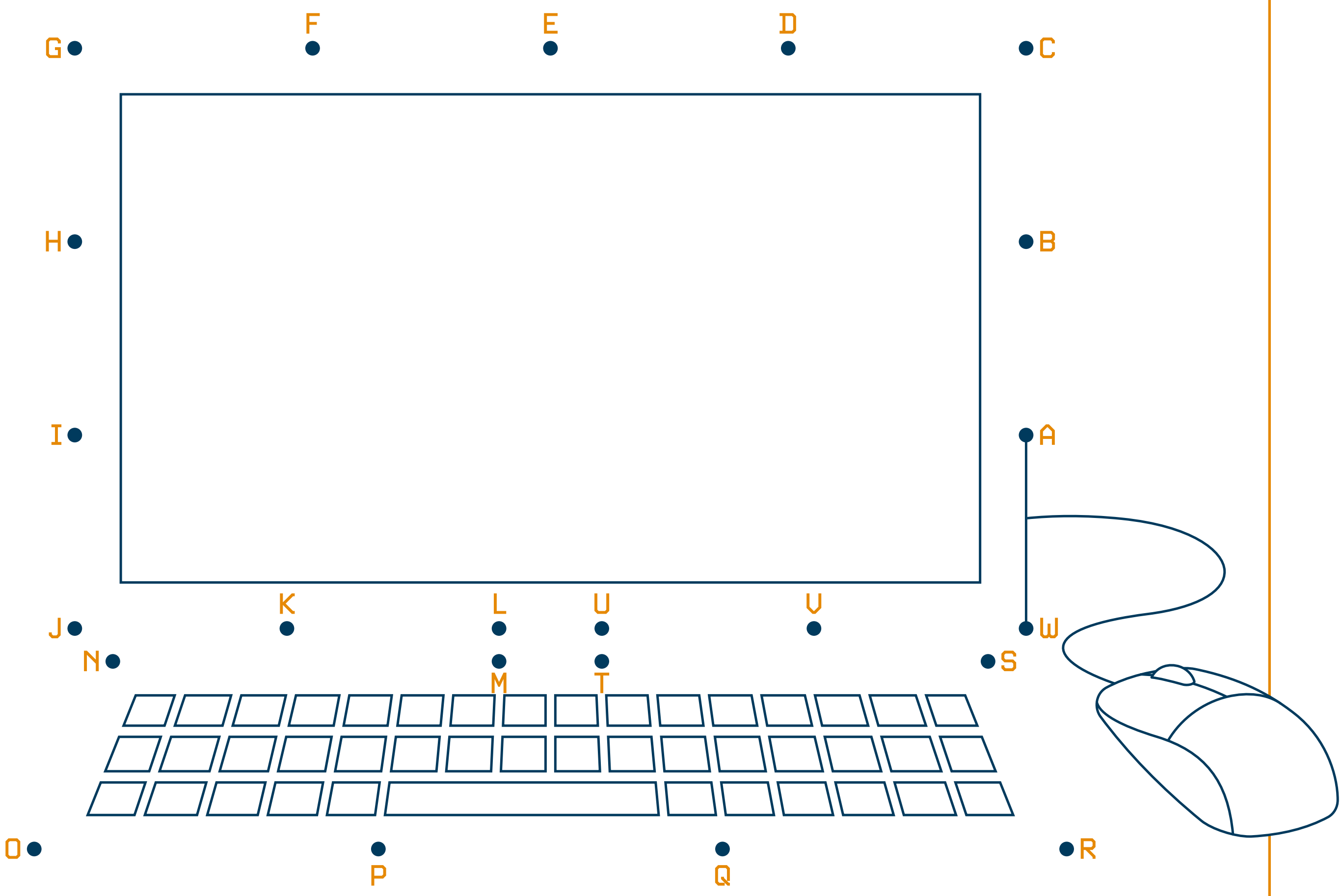
The internet is a vibrant place. Let's bring some color to the World Wide Web!



CONNECT THE DOTS!

Instructions

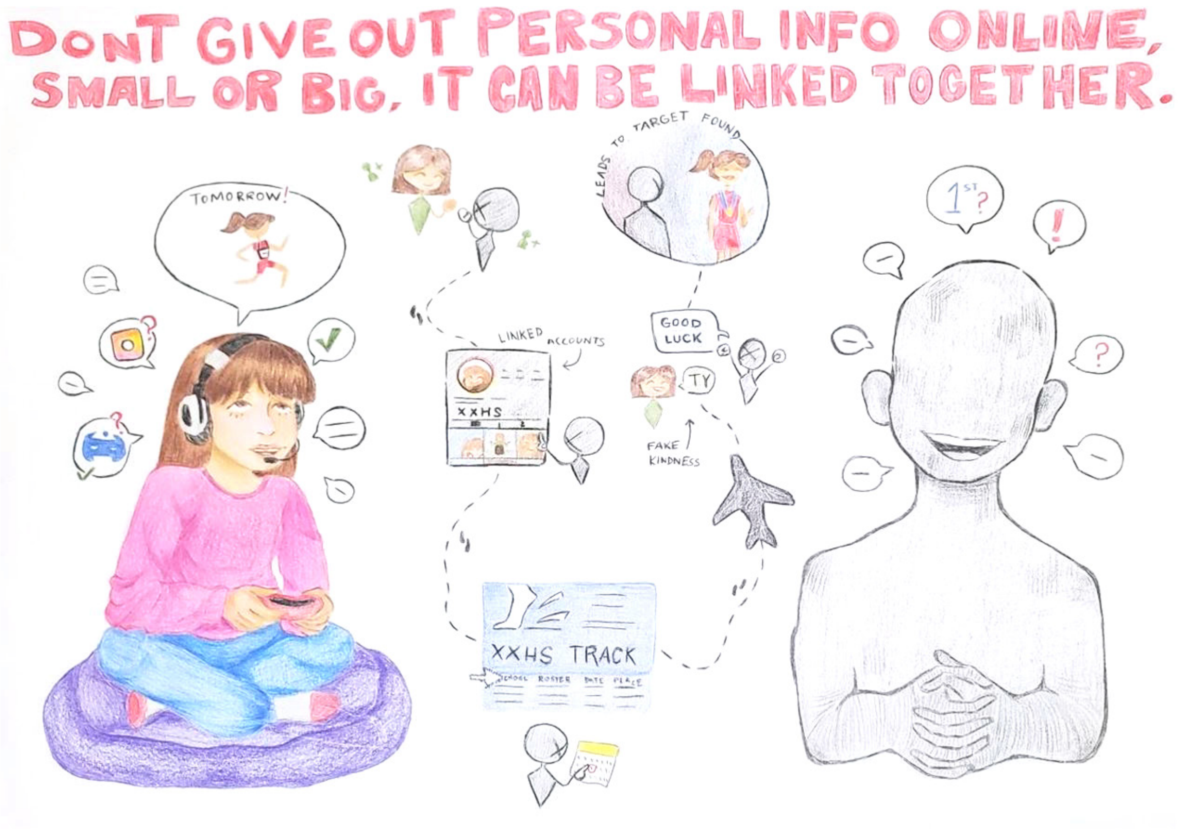
Connect the dots to draw something you'd use to surf the web!



2022 Poster Contest Winner / 2nd Place

Maylin

12th Grade • New York



Cyber Tip

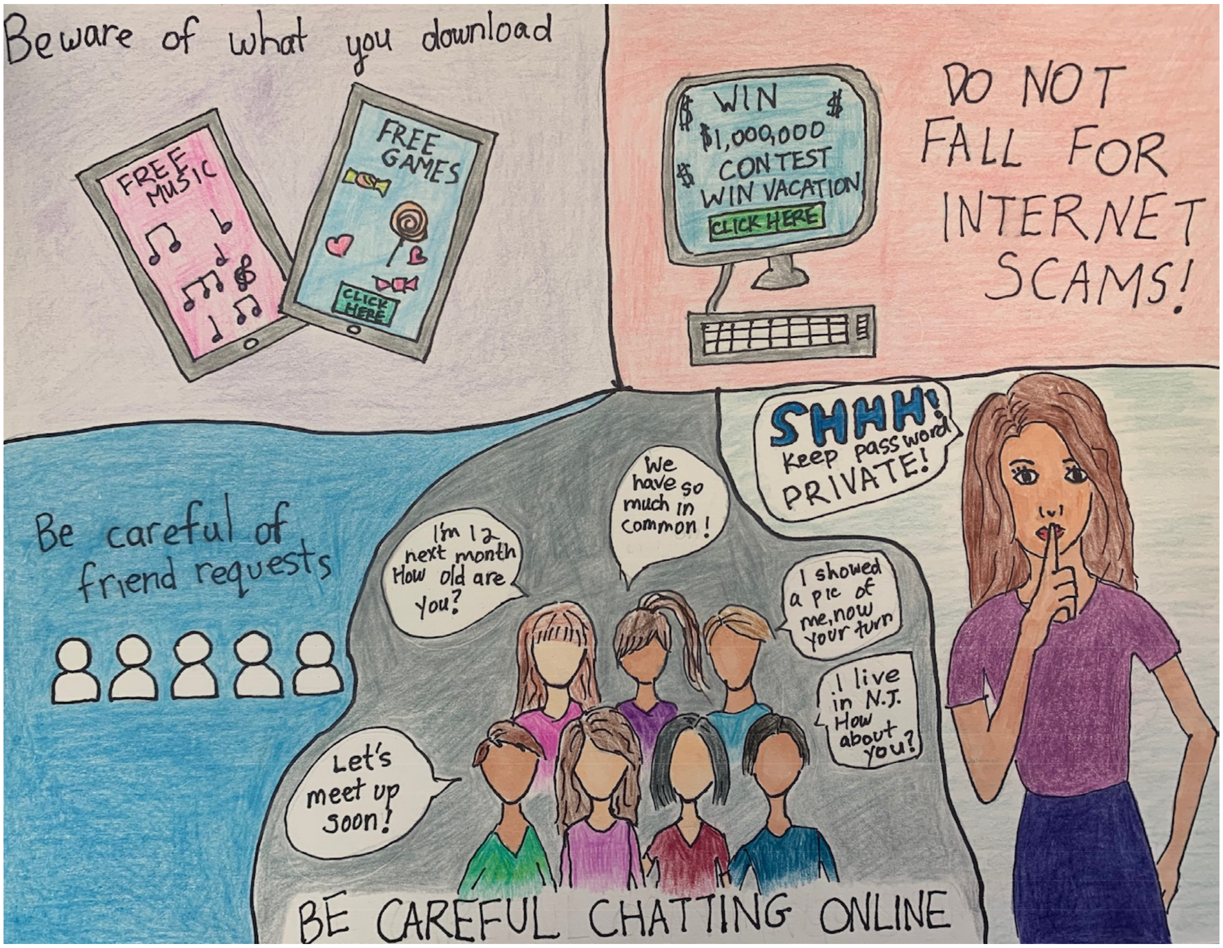
GET PERMISSION

Always get permission from your parent/guardian or, if you're at school, a teacher before using a computer, especially when going online. Some users and websites on the internet may try to steal your information and/or infect your device(s) with malware.

2022 Poster Contest Winner / 3rd Place

Megan

5th Grade • New York


Beware of what you download
FREE MUSIC
FREE GAMES
CLICK HERE
WIN $1,000,000 CONTEST
WIN VACATION
CLICK HERE
DO NOT FALL FOR INTERNET SCAMS!
SHHH! Keep password PRIVATE!
Be careful of friend requests
We have so much in common!
I'm 12 next month How old are you?
I showed a pic of me, now your turn
I live in N.J. How about you?
Let's meet up soon!
BE CAREFUL CHATTING ONLINE

Cyber Point

UNDERSTANDING THE DARK WEB

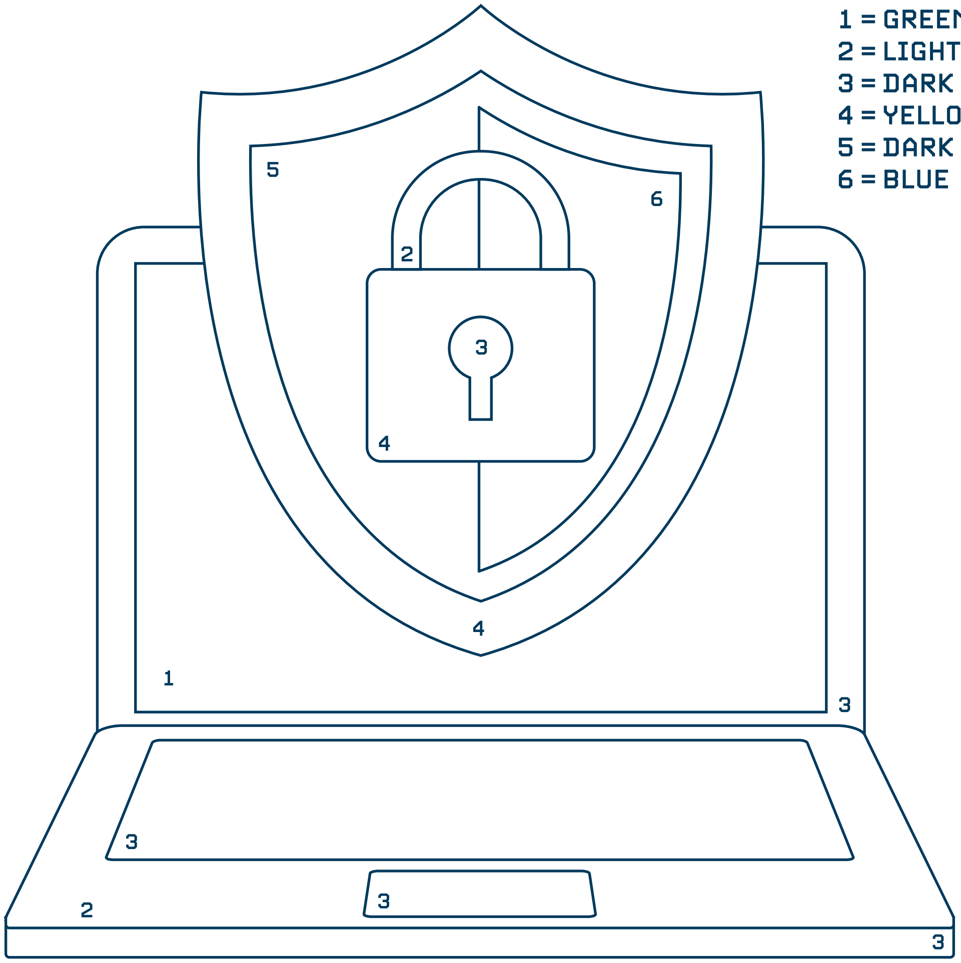
Not everything on the dark web is dangerous. But the dark web is home to many sites where attackers can sell and purchase your sensitive information.

COLOR BY NUMBERS!

Instructions

Use the numbers to color in this representation of cybersecurity.

KEY:
1 = GREEN
2 = LIGHT GRAY
3 = DARK GRAY
4 = YELLOW
5 = DARK BLUE
6 = BLUE

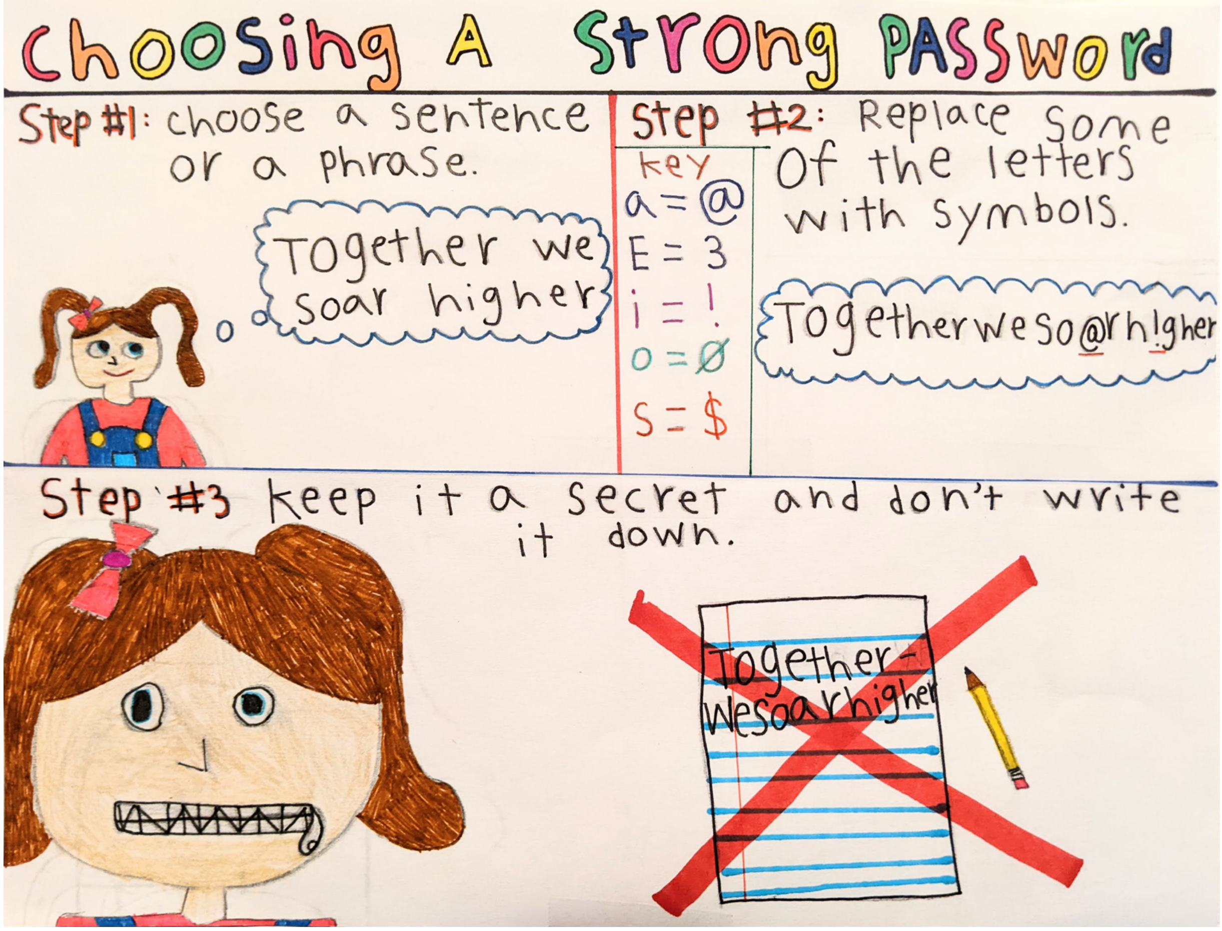


All of us have information we don’t want to fall into the wrong hands.
That’s why it’s never too early to start caring
about your information’s security.

2022 Poster Contest Winner / 4th Place

Leila

3rd Grade • Virginia


Choosing A Strong PASSword
Step #1: choose a sentence or a phrase.
Together we soar higher
Step #2: Replace some of the letters with symbols.
key
a=@
E=3
i=!
o=Ø
S=$
Togetherweso@rh!gher
Step #3 keep it a secret and don't write it down.
Together-wesoarhigher

Cyber Tip

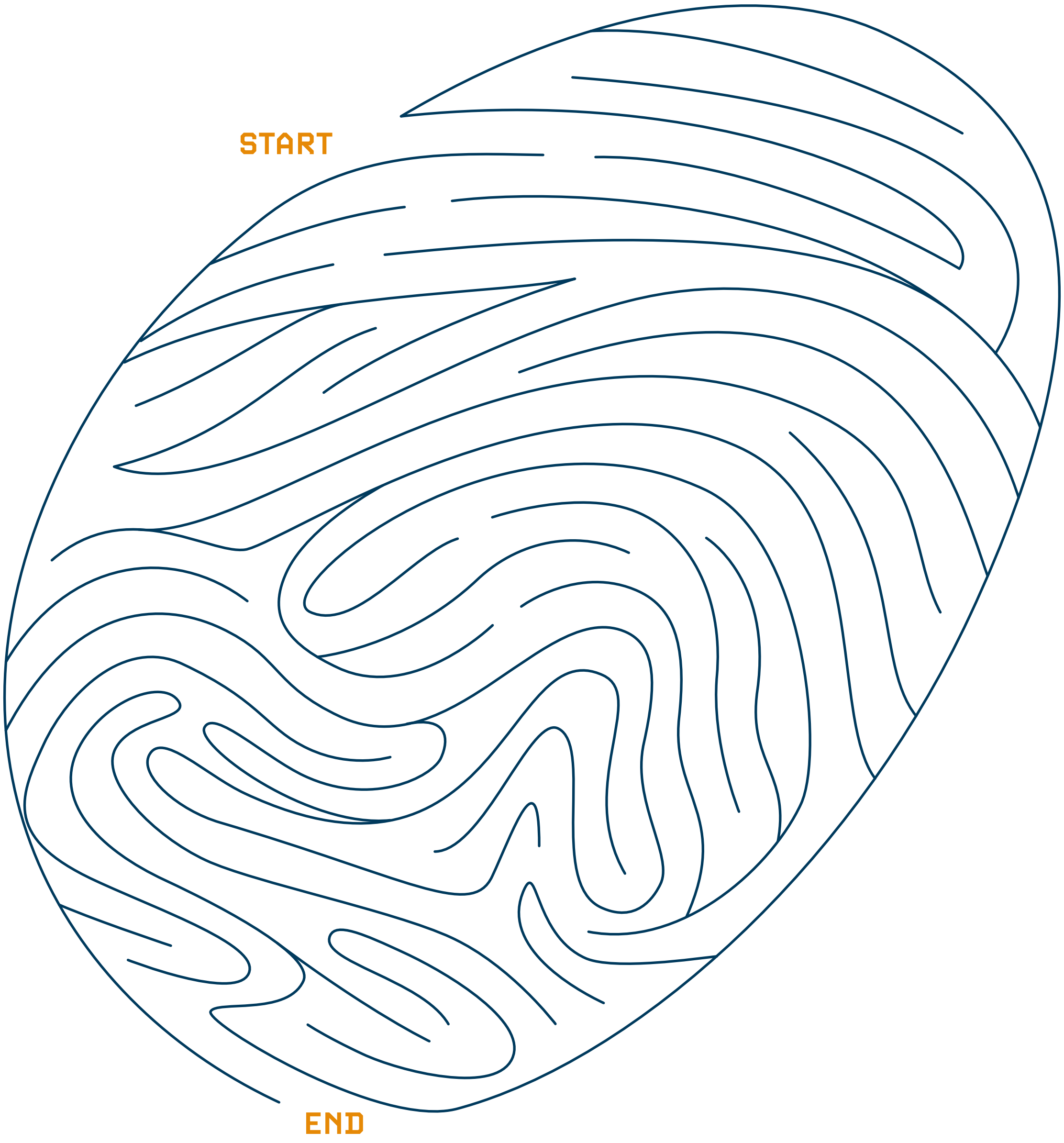
KEEP YOUR PASSWORDS PRIVATE!

Your password is your secret weapon to keep your information safe. Use passwords that are hard to guess. Even better, use a "passphrase" instead! It will be longer, so more secure, and easier to remember, too. Something like "Mystinkydogiswhite." You can also mix numbers with letters and use unique (wrong) spellings, like this: Myst1nkyd0g1zwite!

ESCAPE THE MAZE!

Instructions

Find your way out of this "unique" maze. There's only one
like it in the world—and yours is different too!

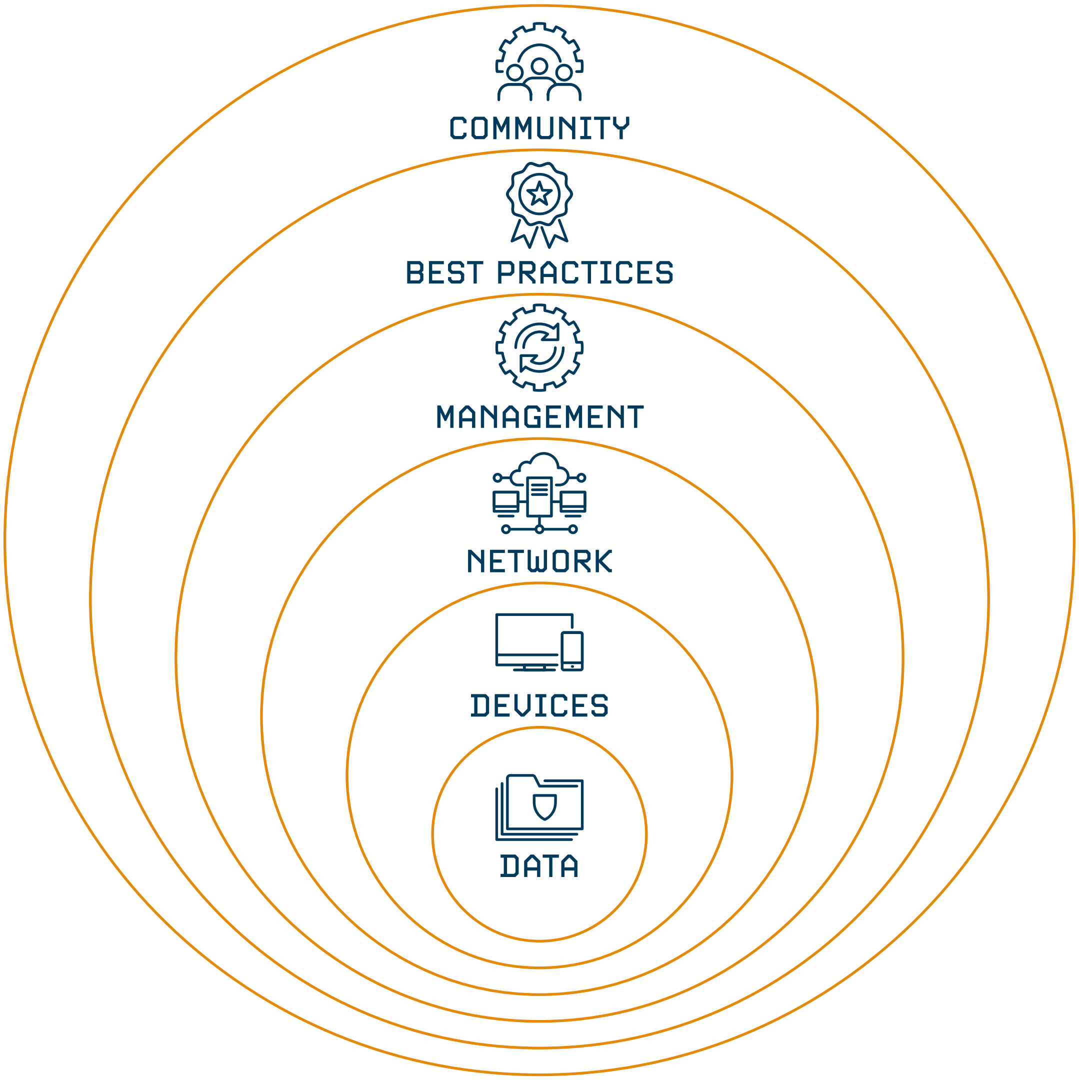


COLORING

Instructions

Color in this picture and learn more about one of the key principles of cybersecurity.

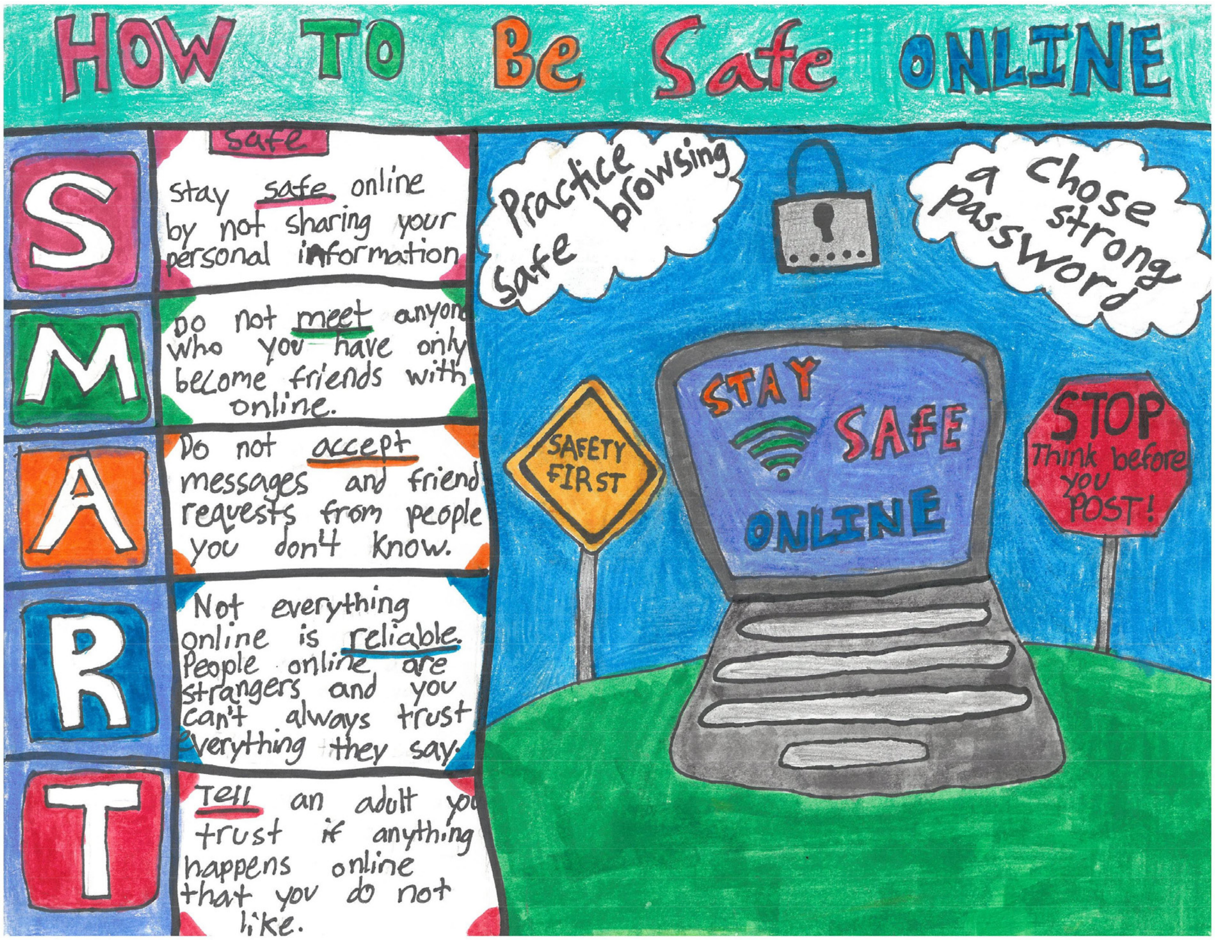
We want our information's security to be like an onion. Peel back one layer, and there's another layer keeping us safe. That's what we call "defense in depth."



2022 Poster Contest Winner / 5th Place

Valentina

5th Grade • New York


HOW TO Be Safe ONLINE
Safe
S
Stay safe online by not sharing your personal information
M
Do not meet anyone who you have only become friends with online.
A
Do not accept messages and friend requests from people you don't know.
R
Not everything online is reliable. People online are strangers and you can't always trust everything they say.
T
Tell an adult you trust if anything happens online that you do not like.
Practice safe browsing
Chose a strong password
SAFETY FIRST
STAY SAFE ONLINE
STOP Think before you POST!

Cyber Point

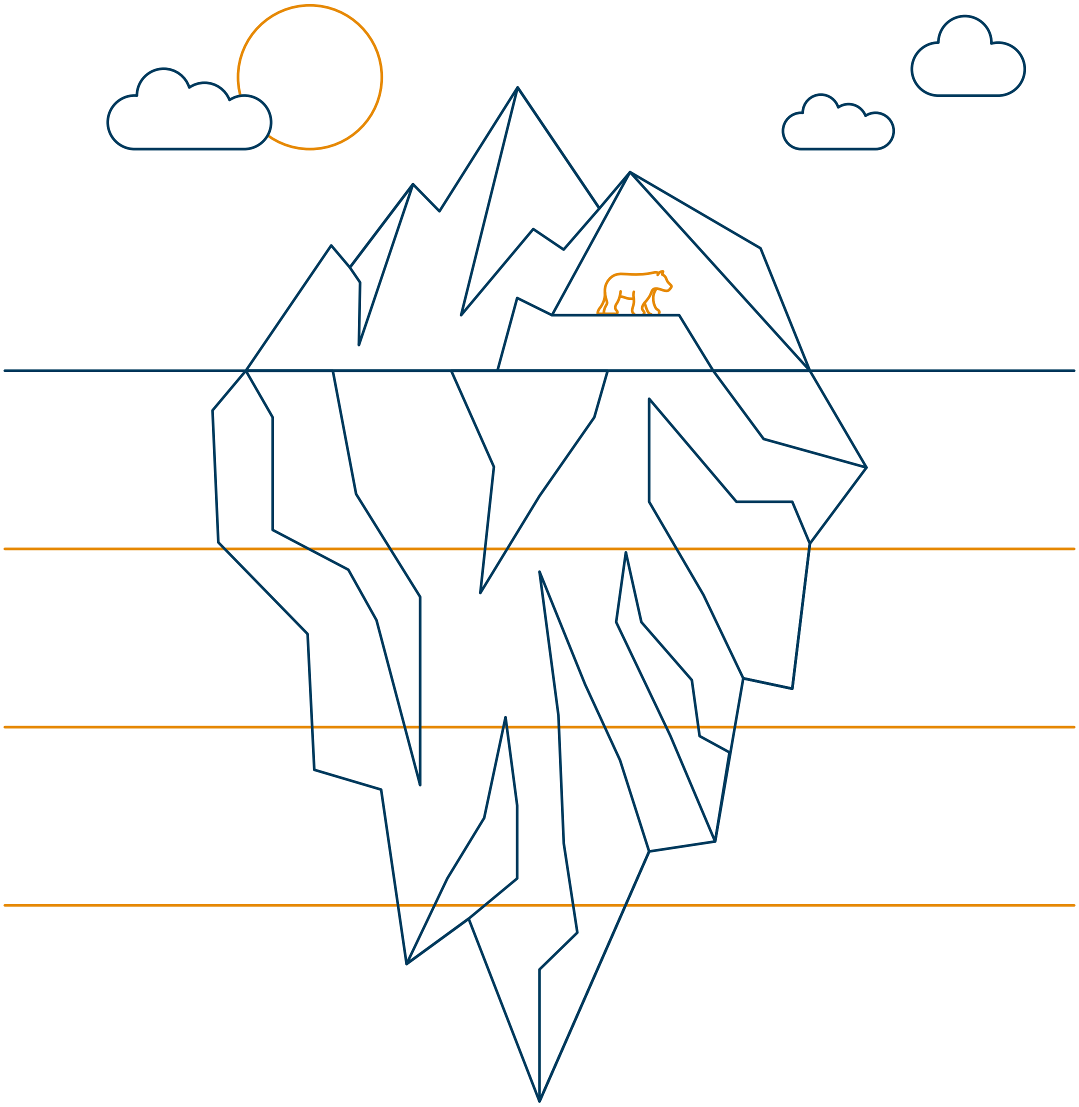
IT'S A WIDE WEB OUT THERE

There's more to the internet than what you can find on Google. In fact, the web extends much deeper than that. There are other levels where attackers buy and sell stolen information, gain access to malicious software, and lay the groundwork for threatening you on the surface web.

COLORING

Instructions

Color in this representation of the internet.
Remember: It gets darker the more you go beneath the surface.



CRACK THE CODE!

Instructions

The cipher below reveals that J = C. This means that each decoded letter is seven letters earlier in the alphabet than each encoded letter. Use this pattern to decode the secret message.

JYFWAVNYHWOF NVLZ ILFVUK JVTWBALYZ.

C___________ ____ ______ C________,

IBA JVTWBALYZ THRL LUJVKLK ZLJYLAZ

___ C________ ____ __C____ __C____

TVYL KPMMPJBSA AV JYHJR.

____ _____C___ __ C__C_.

Cyber Point

Cryptography goes beyond computers. But computers make encoded secrets more difficult to crack.

TEST YOUR KNOWLEDGE!

Instructions

Circle the letter next to the best response to stay safe in the following scenarios.

Question 1

I'm online and I meet someone my age in a chat room. Is it OK to give him or her my address or phone number so we can get together?

a) No. They might be lying about their age to trick you into handing over your information.

b) Yes. If they're the same age, there's no big deal!

c) Maybe. But only if they give you their address and phone number first.

Question 2

I'm visiting a site from a company that I've heard of. They want my name and phone number so I can enter a contest. Is it OK to enter?

a) No, I should not enter any personal information wthout getting a parent or guardian's approval.

b) Yes, it's a contest that seems real.

c) Maybe.

Question 3

You are online and suddenly you come across a video that upsets you or is too violent to watch. What would you do?

a) Do nothing. It was upsetting, but I'll forget about it.

b) Tell a parent or teacher right away.

c) I'm not sure.

UNJUMBLE THE WORDS!

Instructions

Figure out which cybersecurity terms these jumbled letters spell.
Check out the glossary if you need some help!

AYCPRRYOGPHT ____________________

EOTNIPCYNR ____________________

TTPSH ____________________

ADTA ____________________

LRWDO EDWI BEW ____________________

USGIIHN ____________________

CRYMERBIEC ____________________

MSAC ____________________

SMIRNTEAG ____________________

SRGUINF ____________________

IAOICNPLTAP ____________________

WORD SEARCH

Instructions

Can you find all the following terms in the word search below?

The OSI model stands for Open System Interconnection model. It provides a view of all the different layers that factor into cybersecurity.

Find and circle each layer name in the grid below: **physical**, **data link**, **network**, **transport**, **session**, **presentation**, and **application**.

Words can go in any direction and share the same letters where they cross over each other.

L	Y	N	O	B	O	O	Y	P	R	T	P
D	A	T	A	L	I	N	K	H	A	R	L
P	J	P	P	M	W	W	O	Y	E	N	I
R	K	X	P	W	S	E	S	S	I	O	N
N	J	N	L	H	R	R	E	I	O	N	C
L	A	C	I	S	Y	N	P	C	U	I	I
A	P	V	C	A	T	W	O	A	E	E	M
D	U	T	A	A	P	T	R	L	Y	O	N
S	A	K	T	R	A	N	S	P	O	R	T
Y	X	I	I	D	F	A	T	U	K	S	P
T	O	R	O	P	S	N	A	R	T	U	L
N	T	E	N	E	T	W	O	R	K	N	K

MATCH THE VOCABULARY!

Instructions

Draw a line from the vocabulary term to its correct definition.

- HTTP
- Data Breach
- Multi-Factor Authentication (MFA)
- Password
- Phishing
- Passphrase
- Whaling
- Cybersecurity

a) A cyber attack that results in the exposure of information.

b) An attempt to trick people into visiting malicious websites and/or sharing their personal information via email.

c) A string of characters that helps with authenticating a user during a login process.

d) The use of people, processes, and technology to defend against cyber attacks and other digital threats.

e) Short for "Hypertext Transfer Protocol." It's central for communicating data over the internet.

f) A sequence of words or text for securing access to a trusted account.

g) A form of phishing that specifically targets senior people in an organization, like the CEO orother executives.

h) A method of identity and access management that requires a user to provide multiple factors of authentication as part of the login process.

2022 Poster Contest Winner / 6th Place

Eliana

12th Grade • New York

WHO KNOWS WHO IS TRACKING YOUR LOCATION
Y/N
@LA
1 min ago
@eiffel tower
Y/N
location: 317 XX ST
44 AVE
XX ST
317
ON'T SHARE YOUR LOCATION WITH STRANGE

Cyber Tip

USE HTTPS!

Make sure you use HTTPS when you're submitting sensitive information like a password online. You can do this by clicking in the browser's address bar, or where you type in the websites you want to visit. If the site is using HTTPS, you'll see "https" all the way to the left along with a lock icon.

WHICH -WARE?

Instructions

Match each "-ware" term from the glossary with the correct definition.

MALWARE	a) A type of threat that uses social engineering techniques to trick people into buying or downloading something useless or malicious.
ADWARE	b) A type of malware that encrypts a victim's information and demands money in exchange for a recovery key.
SPYWARE	c) Programs that display an advertisement on the screen. They are often installed without the user realizing.
RANSOMWARE	d) Short for "malicious software." Programs that damage computers, steal personal information, or expose a computer to further damage by crackers.
SOFTWARE	e) The physical components of a computer system, like the wiring, monitor, laptop, or disc drive.
HARDWARE	f) A piece of software that's embedded in a piece of hardware.
FIRMWARE	g) Programs that run on your computer.
SCAREWARE	h) A type of malware designed to monitor victims without their knowledge.

TEST YOUR KNOWLEDGE!

Instructions

Choose the best response to stay safe in the following scenarios.

Question 1

I'm in the middle of a chat session and someone says something really mean. Should I:

a) Say something mean back. They deserve it.

b) Tell them to apologize.

c) Don't respond and let a trusted adult know if it bothers me.

Question 2

I'm online and I get a message from my internet provider asking for my password. They say they need it to fix my account. Should I give it to them?

a) Yes, if something is wrong with my account. I should do whatever I can to fix it.

b) No, Internet Service Providers (ISPs) will never ask you for your password information.

c) Maybe, if the grammar is correct and the request seems real.

Question 3

One of your friends wants to do a viral challenge they saw online that involves doing a dangerous stunt. What do you do?

a) Do the challenge. It's risky but could pay off and make you famous online.

b) Only do it if you are the one recording and someone else does the stunt.

c) Explain to them why it's not a good idea to perform stunts for internet visibility.

MATCH THE VOCABULARY!

Instructions

Draw a line from the vocabulary term to its correct definition.

a) User-facing software that runs on a personal computing device. Common examples include web browsers and computer games.

b) A social network that is used to share personal images and information.

c) Principles of behaving ethically online.

d) The part of a social networking site that allows you to control who sees information about you.

e) A crime that involves someone obtaining personal information such as a credit card or bank account number from someone else in order to steal money or commit other harmful acts.

f) A form of phishing that uses SMS as its delivery vector.

g) A type of malware that impersonates a legitimate program to trick users into installing it on their devices.

h) An unsolicited advertisement.

i) Software that uses vulnerabilities to infect computing devices with viruses, malware, and other threats.

j) Something fraudulent that's designed to cheat a victim out of something.

Identity Theft

Pop-up

Social Media

Netiquette

Privacy Settings

Trojan

Scam

Application

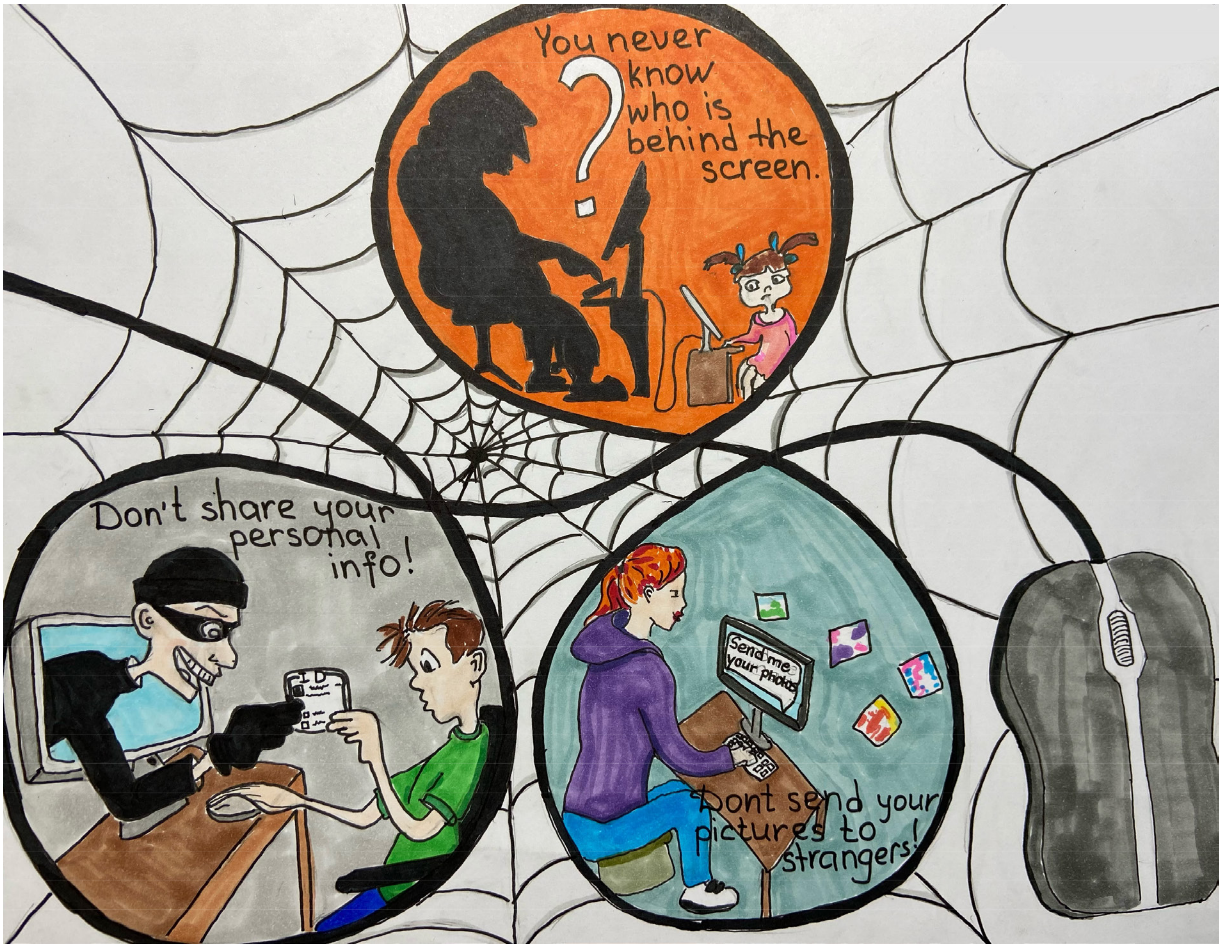
Smishing

Exploit Kit

2022 Poster Contest Winner / 7th Place

Alisa

7th Grade • New York


You never know who is behind the screen.
Don't share your personal info!
ID
Send me your photos
Dont send your pictures to strangers!

UNJUMBLE THE WORDS!

Instructions

Instructions: Figure out which glossary terms these jumbled letters spell.

ITYETIDN FDARU ______________________

DOAUPL ______________________

LCBRUYLBEY ______________________

GIIAFTNCHS ______________________

SIRGLNVIMAET ______________________

LEIRTNLABVIYU ______________________

PSRSHASPAE ______________________

BICIKLTCA ______________________

AWDNDLOO ______________________

HOW TO STOP CYBERBULLYING IN ITS TRACKS

According to Security.org, 21% of children between the ages of 10 and 18 have been a victim of cyberbullying. More than half (56%) of those cases occurred between January 2020 and July 2020, during the height of the COVID-19 lockdowns.

You can stop cyberbullying by taking these steps:

Step 1

Save any evidence of the cyberbullying.

Step 2

Block the cyberbully on the platform they used to commit the cyberbullying.

Step 3

Log off from the computer.

Step 4

Tell a parent, guardian, or teacher.

Here are tips to avoid becoming a bystander to cyberbullying:

Tip 1

Don't join into instances of bullying online.

Tip 2

Respond privately to the cyberbully and vocalize how you don't support what they did.

Tip 3

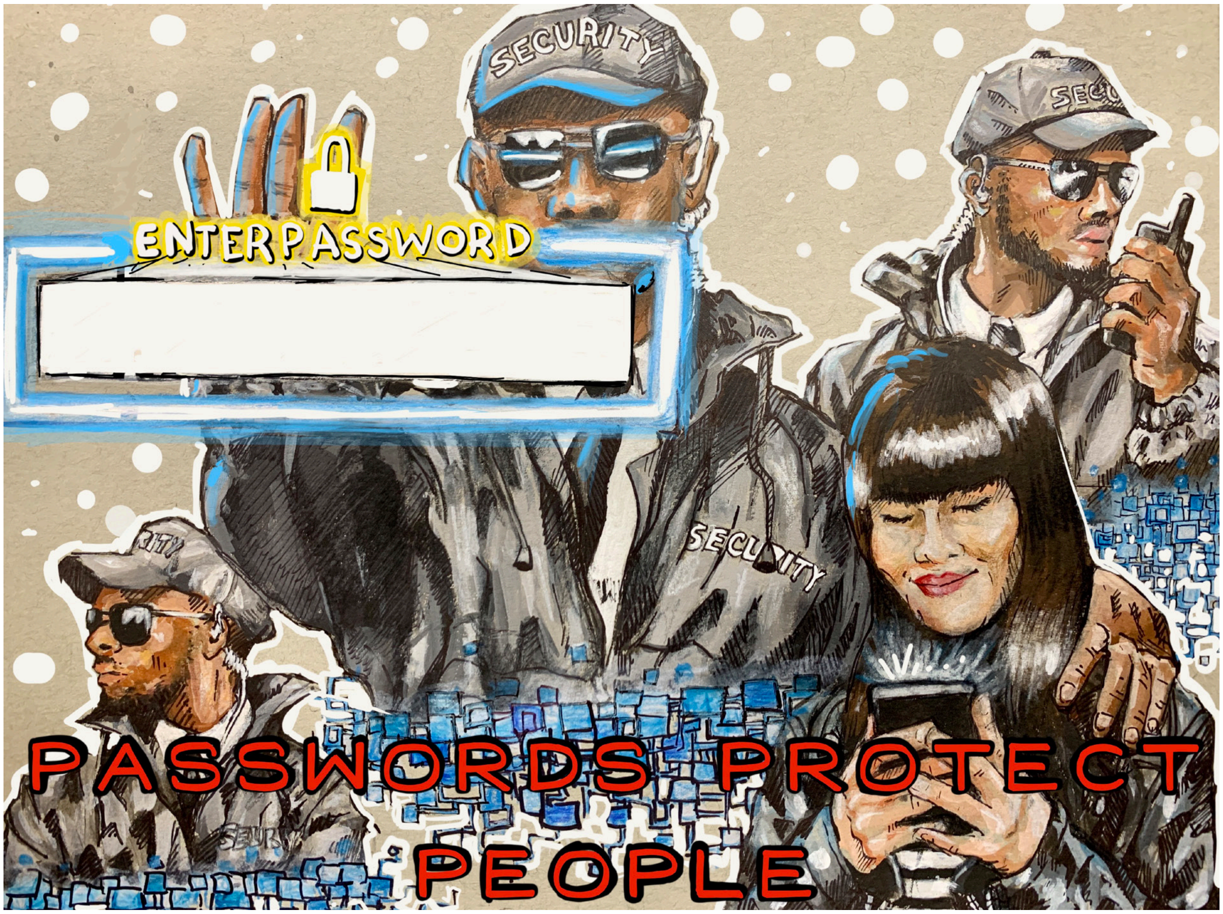
Respond privately to the victim and show your support for them.

Cyberbullying causes victims to feel angry, hurt, and bad about themselves. Instances of cyberbullying can also hurt victims' relationships and physical health.

2022 Poster Contest Winner / 8th Place

Jacob

11th Grade • Texas



ANTI-PHISHING TIPS

In the first quarter of 2022, the Anti-Phishing Working Group (APWG) observed 1,025,968 total phishing attacks. This is the highest volume of phishing attacks APWG has detected to date.

Common signs of phishing attacks include the following:

Example 1

Requests for payment information

Example 2

Requests for personal details

Example 3

Offers that appear too good to be true

Example 4

Extensive hyperlinks in emails

Here's how to defend against a phishing attack:

Example 1

Don't reply to the email

Example 2

Don't click on any embedded links or email attachments

Example 3

Report the email to parent/ guardian/teacher

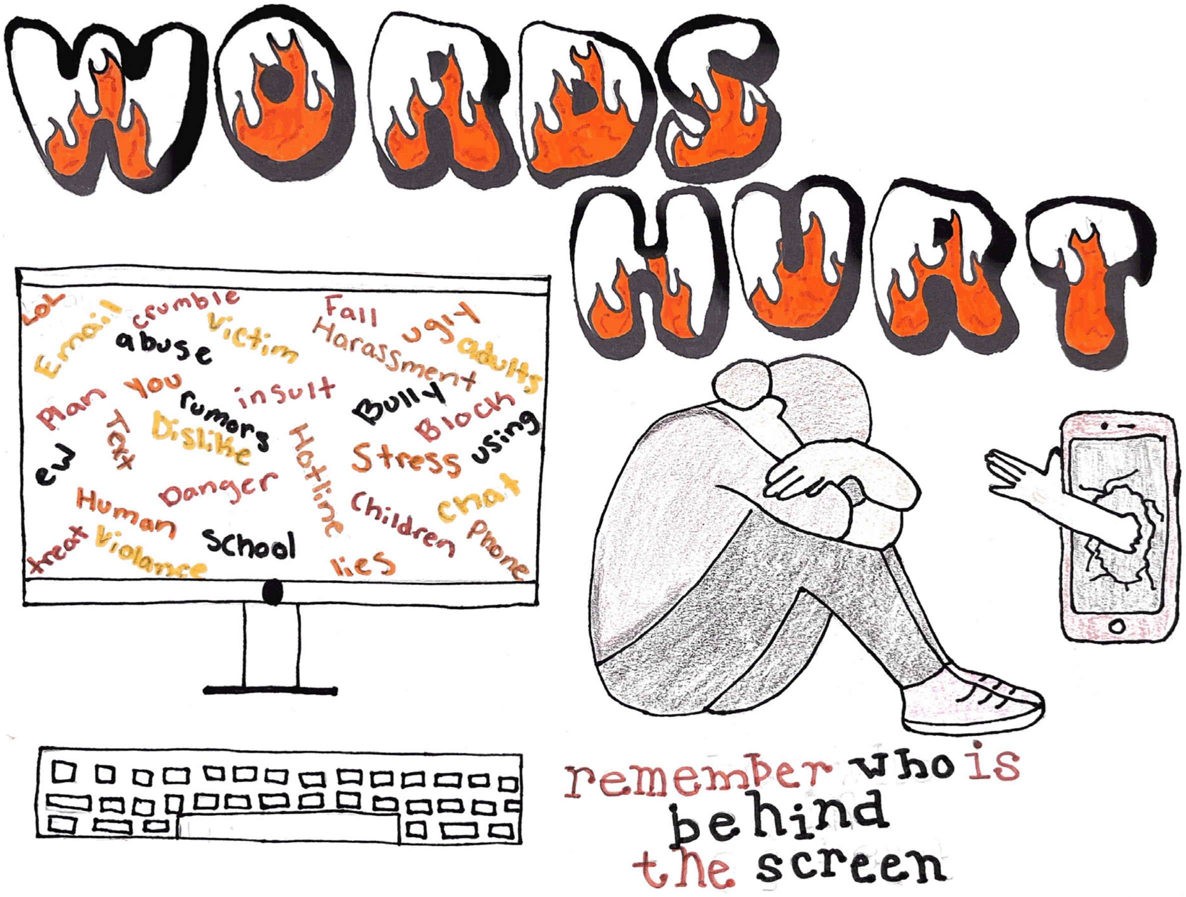
Example 4

Delete the email

2022 Poster Contest Winner / 9th Place

Teagan

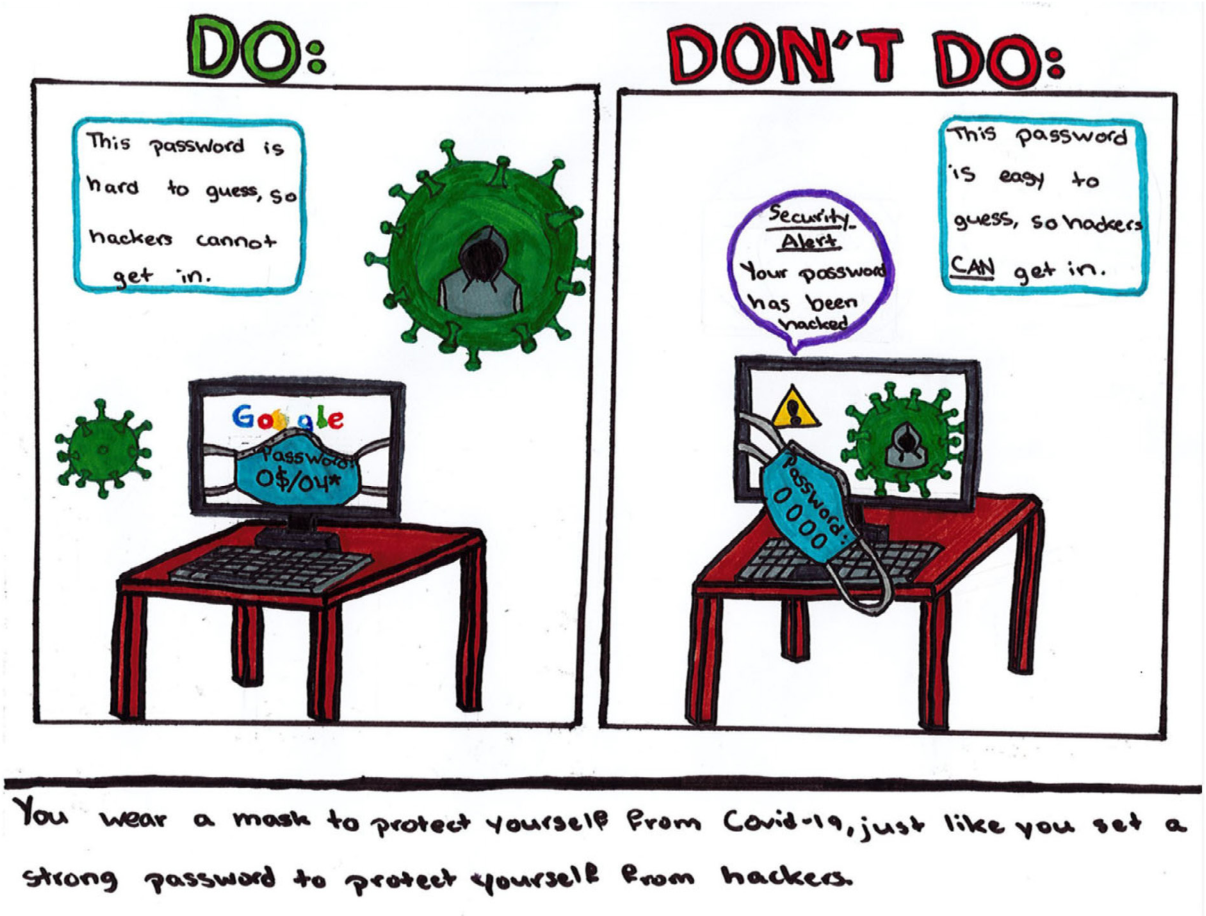
7th Grade • South Dakota



2022 Poster Contest Winner / 10th Place

Layan

6th Grade • Pennsylvania


DO:
This password is hard to guess, so hackers cannot get in.
Google
Password: O$/04*
DON'T DO:
Security Alert
Your password has been hacked
This password is easy to guess, so hackers CAN get in.
Password: 0000
You wear a mask to protect yourself from Covid-19, just like you set a strong password to protect yourself from hackers.

MATCH THE VOCABULARY!

Instructions

Draw a line from the vocabulary term to its correct definition.

Security Settings

Social Engineering

Identity Fraud

Man-in-the-Middle (MitM) Attack

Information Security

Malvertising

Dark Web

MMS

Troll

Cookie

a) A type of cyber attack that manipulates human users into doing something that weakens their cybersecurity like sharing sensitive data.

b) Part of the deep web that relies on connections made between trusted peers. It is not automatically accessible by ordinary users.

c) A cyber attack in which a malicious actor is able to eavesdrop on the communications between two parties.

d) The part of a social networking site that allows you to control who sees information about you.

f) Short for “malicious advertising,” this is when digital attacks use legitimate advertising networks to spread malware.

g) A process of protecting digital and analog information against unauthorized access, disclosure, and tampering.

h) Short for “multimedia messaging service,” MMS enables mobile uses to exchange images, videos, and other multimedia files with one another.

i) The act of misusing someone’s identifying account(s) or information.

j) Someone who posts upsetting messages or images on social media for the sole purpose of gaining an emotional reaction from the viewers.

k) You can’t eat these, but they DO keep track of your user preferences.

CHOOSE A CYBERSECURITY CAREER PATH

Instructions

Do you have the following skills? If so, you might pursue the associated career path.

Complex problem solving, creativity, strong communication skills

You chose **Cybersecurity Engineer.** Uphold the security of their organization's systems and networks along with the data they store.

Curiosity and insight, ability to write reports and explain the evidence, communication skills

You chose **Cyber Forensics Expert.** Analyze data breaches and other security incidents using digital evidence.

Ability to learn quickly, teamwork, strong written & verbal communication, good ethics

You chose **Ethical Hacker (Penetration Tester).** This is a person who acts with the approval of an organization to evaluate systems and other resources for vulnerabilities.

Planning & organization, problem-solving, analytical, systems thinking

You chose **Security Operations Center Analyst.** The front line of an organization's information security team. They respond to incidents as they happen.

Attention to detail, complex problem solving, systems and software knowledge

You chose **Technical Support Specialist.** An individual who helps customers solve technical issues that affect their use of supported hardware and software.

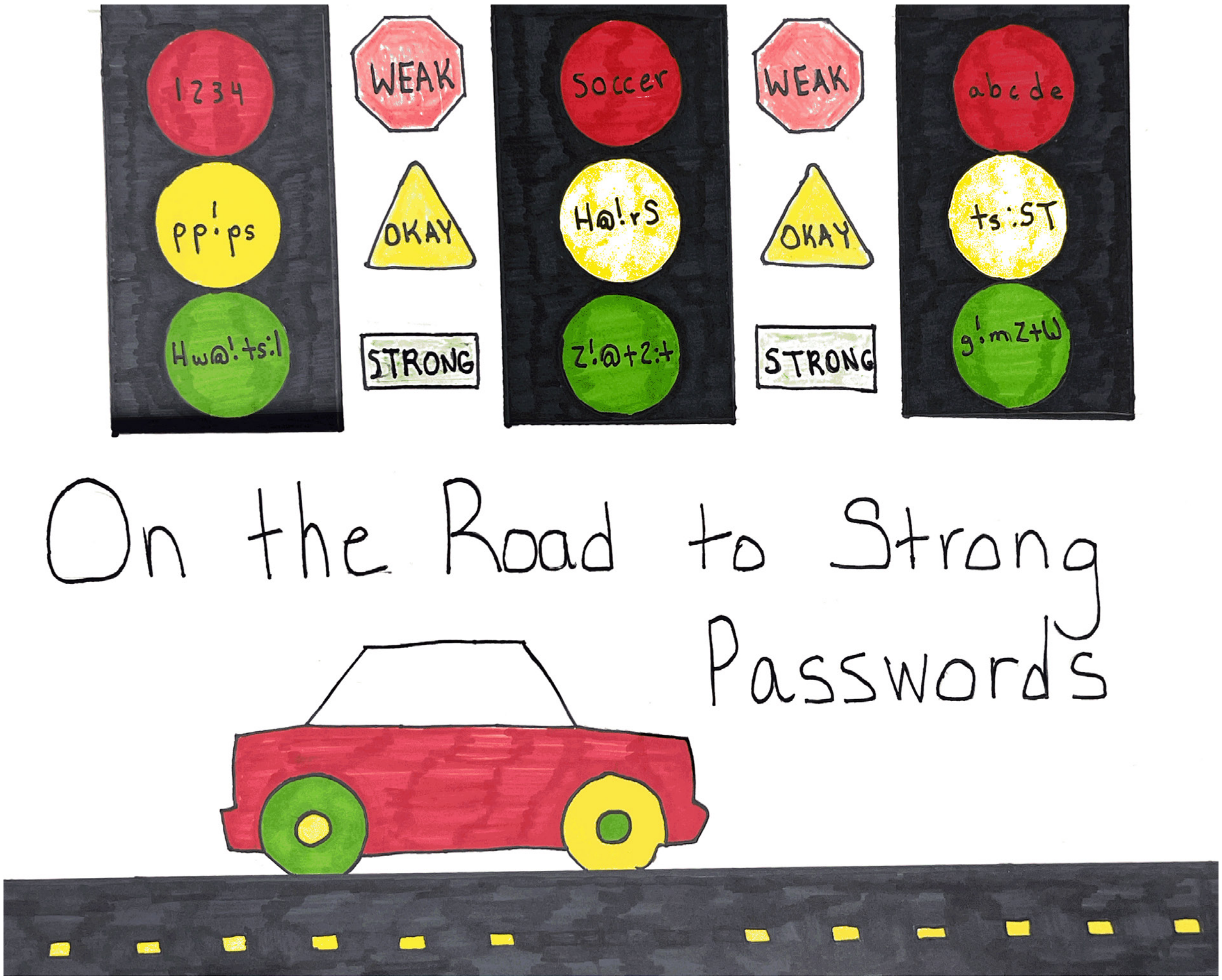
Analytical skills, organization skills, strong leadership and communication qualities

You chose **Systems Administrator.** A professional who's responsible for maintaining and managing computer systems and servers.

2022 Poster Contest Winner / 11th Place

Karlie

7th Grade • South Dakota



TEST YOUR KNOWLEDGE!

Instructions

Choose the best response to stay safe in the following scenarios.

Question 1

You get a new email. It tells you that "you have won $1,000,000 in the lottery. Click this link to claim your prize!!!" Would you open it?

a) No, this is not legitimate – Clicking on links that seem too good to be true with offers or rewards put your personal information in danger and your computer in danger of getting infected with a virus.

b) Yes, free money!!

c) Maybe, it could be real.

Question 2

If your friend asks you for your login ID and password to use your online account for some time, what would you do?

a) Give it to them.

b) Don't give it to them – You should never give out your passwords OR log-ins to anyone, even if it's a very close friend. This information should always be kept private.

c) Maybe. If we are really close, it might be okay to share this.

Question 3

You are on Facebook when you get a message and a friend request from someone you don't know. What would you do?

a) Delete the request and tell a parent or teacher. You don't know them and you should always treat strangers online the way you do in real life, with caution.

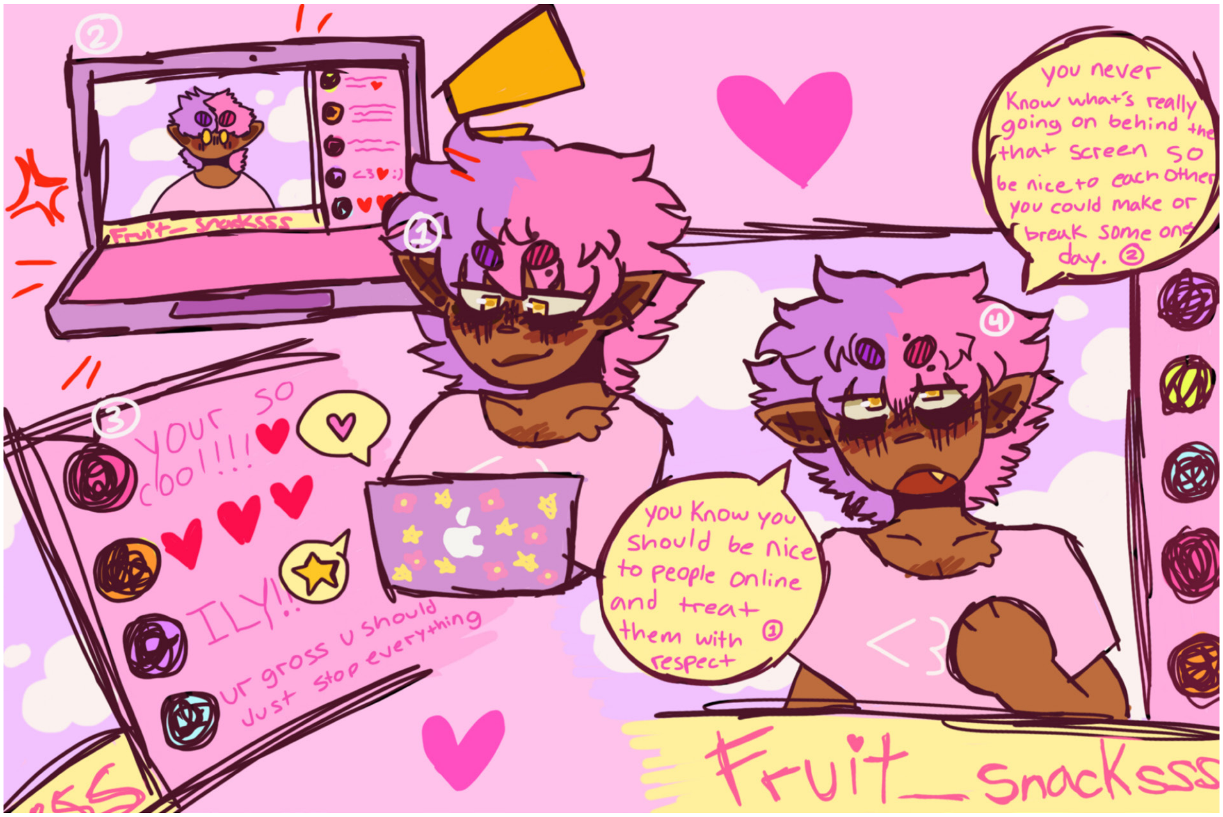
b) Accept! The more friends, the better.

c) It depends. It could be a mutual friend.

2022 Poster Contest Winner / 12th Place

Ana Alicia

8th Grade • Texas


②
Fruit_snacksss
<3 ♥ :)
①
you never Know what's really going on behind the that screen so be nice to each other you could make or break some one day. ②
③
your so cool!!!!
ILY!!
ur gross u should just stop everything
ssS
④
you Know you should be nice to people online and treat them with ① respect
<3
Fruit_snacksss

PLAN FOR A FUTURE IN CYBERSECURITY

Instructions

Use these resources to get the practical skills you need for a career in cybersecurity.

CyberStart America

A free cybersecurity training game designed for high school students. Players can win college scholarships by participating.

https://www.cyberstartamerica.org/

CyberAces

Offers tutorials and courses and maintains users and groups for professionals to access.

https://www.sans.org/cyberaces/

Cybrary.it

Offers free courses in cybersecurity courses like vulnerability management, malware analysis, and IT/security fundamentals.

https://www.cybrary.it/

CompTIA CertMaster Learn

Helps you master the skills covered by CompTIA certifications.

https://www.comptia.org/training/certmaster-learn

Udemy

Provides access to free classes on cybersecurity fundamentals, coding, and a host of other technology-focused topics.

https://www.udemy.com/

U.S. Cyber Challenge

Program that uses online competitions and week-long cybersecurity training to find tomorrow's cybersecurity workforce.

https://www.uscyberchallenge.org/

The SANS Institute

Offers training and cyber security certifications.

https://www.sans.org/

Center for Internet Security

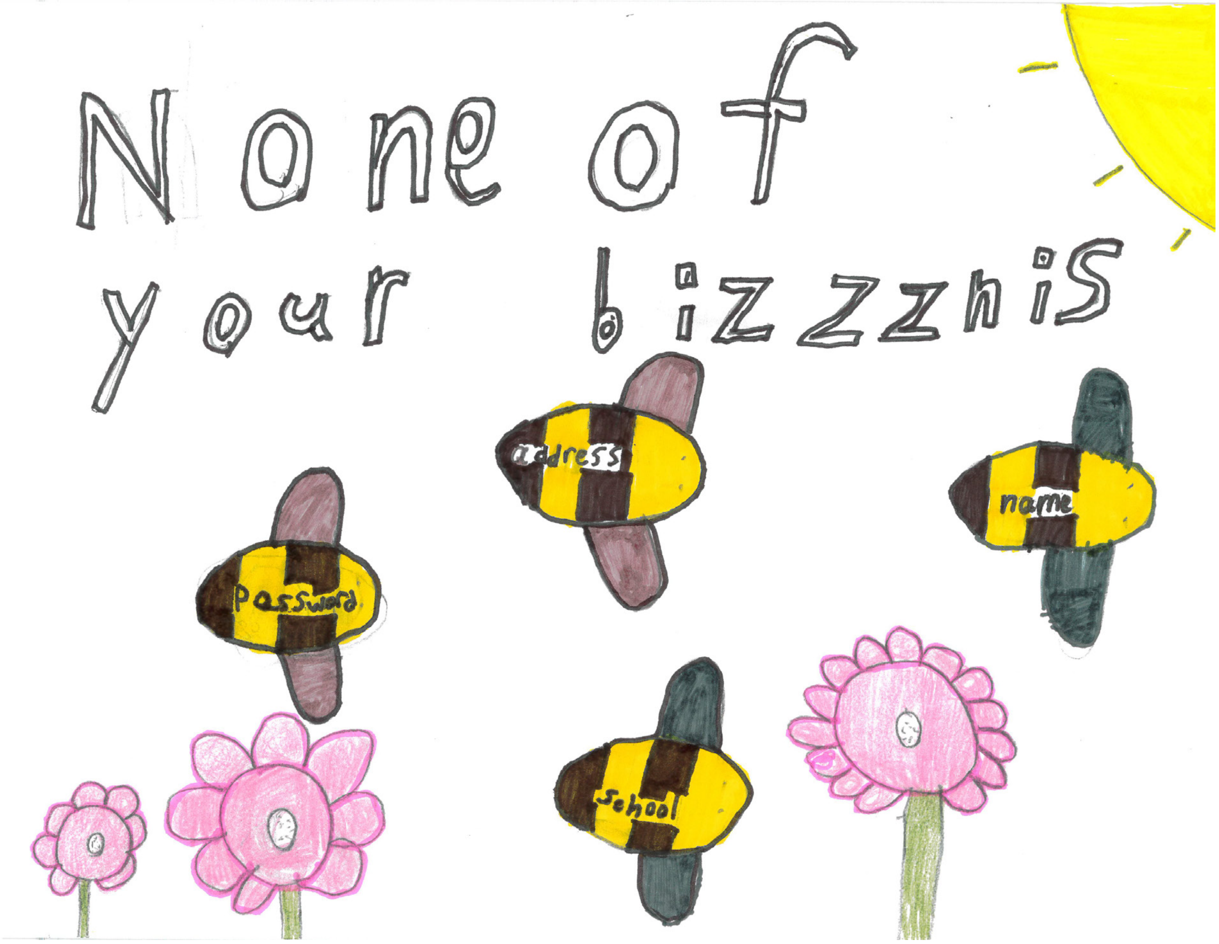
Publishes blogs and insights concerning zero trust, supply chain security, and other important concepts.

https://www.cisecurity.org/

2022 Poster Contest Winner / 13th Place

Atikiss

4th Grade • Montana



WHICH -ISHING?

Instructions

Match each "-ishing" term from the glossary with the correct definition.

CATFISHING

PHISHING

SMISHING

VISHING

a) An attempt to trick people into visiting malicious websites and/or sharing their personal information via email.

b) A form of phishing that uses voice-based phone calls as its delivery vector.

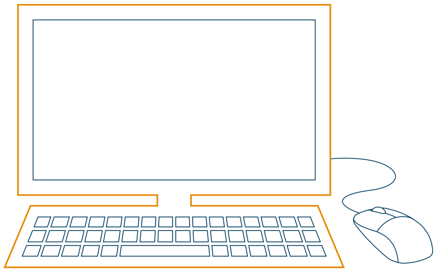
c) Luring someone into a relationship either through a chatroom or social media website using a fake identity.

d) A form of phishing that uses SMS as its delivery vector.

GAME OVER

Answer Key

Page 6 // Connect the Dots



Page 11 // Escape the Maze!

Page 15 // Crack the Code

CRYPTOGRAPHY GOES BEYOND COMPUTERS, BUT COMPUTERS MAKE ENCODED SECRETS MORE DIFFICULT TO CRACK.

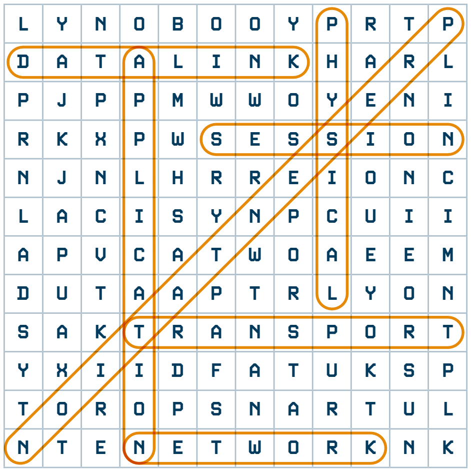
Page 16 // Test Your Knowledge

QUESTION 1: A
QUESTION 2: A
QUESTION 3: B

Page 17 // Unjumble the Words

CRYPTOGRAPHY
ENCRYPTION
HTTPS
DATA
WORLD WIDE WEB
VISHING
CYBERCRIME
SCAM
STREAMING
SURFING
APPLICATION

Page 18 // Word Search



L	Y	N	O	B	O	O	Y	P	R	T	P
D	A	T	A	L	I	N	K	H	A	R	L
P	J	P	P	M	W	W	O	Y	E	N	I
R	K	X	P	W	S	E	S	S	I	O	N
N	J	N	L	H	R	R	E	I	O	N	C
L	A	C	I	S	Y	N	P	C	U	I	I
A	P	V	C	A	T	W	O	A	E	E	M
D	U	T	A	A	P	T	R	L	Y	O	N
S	A	K	T	R	A	N	S	P	O	R	T
Y	X	I	I	D	F	A	T	U	K	S	P
T	O	R	O	P	S	N	A	R	T	U	L
N	T	E	N	E	T	W	O	R	K	N	K

Page 19 // Match the Vocabulary

HTTP: E
DATA BREACH: A
MULTI-FACTOR AUTHENTICATION: H
PHISHING: B
PASSWORD: C
PASSPHRASE: F
WHALING: G
CYBERSECURITY: D

Answer Key

Page 21 // Which -WARE?

MALWARE: D
ADWARE: C
SPYWARE: H
RANSOMWARE: B
SOFTWARE: G
HARDWARE: E
FIRMWARE: F
SCAREWARE: A

Page 22 // Test Your Knowledge

QUESTION 1: C
QUESTION 2: B
QUESTION 3: C

Page 23 // Match the Vocabulary

IDENTIFY THEFT: E
POP-UP: H
SOCIAL MEDIA: B
NETIQUETTE: C
PRIVACY SETTINGS: D
TROJAN: G
SCAM: J
APPLICATION: A
SMISHING: F
EXPLOIT KIT: I

Page 25 // Unjumble the Words

IDENTITY FRAUD
UPLOAD
CYBERBULLY
CATFISHING
MALVERTISING
VULNERABILITY
PASSPHRASE
CLICKBAIT
DOWNLOAD

Page 31 // Match the Vocabulary

SECURITY SETTINGS: D
SOCIAL ENGINEERING: A
IDENTITY FRAUD: I
MAN-IN-THE-MIDDLE ATTACK: C
INFORMATION SECURITY: G

MALVERTISING: F
DARK WEB: B
MMS: H
TROLL: J
COOKIE: K

Page 34 // Test Your Knowledge

QUESTION 1: A
QUESTION 2: B
QUESTION 3: A

Page 38 // Which -ISHING?

CATFISHING: C
PHISHING: A
SMISHING: D
VISHING: B

Cybersecurity Awareness

Kids Safe Online

MS-ISAC® Poster Contest

Getting Started

Public, Private, and home schooled students in Grades K-12 are invited to participate for a chance to have their artwork displayed on the 2023 MS-ISAC Posters and the Kids Safe Online Activity Book! Entries should feature original artwork illustrating the safe use of the Internet and/or mobile devices.

Suggested Topics

Grades K-8

- How should you treat others online?
- What information is safe to put on social media and what should you keep private?
- How should you handle unwanted attention or strangers online?
- How can you select a strong password and keep it secure?
- How can you handle cyberbullying?

Grades 9-12

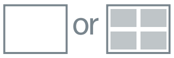
- How can you preserve your online reputation or "digital footprint" on both social media and elsewhere on the Internet?
- How should you handle unwanted attention or strangers online?
- How can you select a strong password and keep it secure?
- Why is it important to keep your devices and software up to date?
- When is it safe to text and what information is safe to text?

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Helping Keep Kids Safe Online

Format

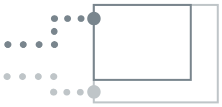
- Original hand-drawn or electronically created submissions will be accepted. Hand-drawn submissions must be scanned.
- Text should be dark and large enough to read.
- Submissions may be in the format of either a full-page drawing or a 4-panel comic.



Layout & Dimensions

Only landscape layout submissions will be accepted!

- Minimum: 11" x 8.5"
- Maximum: 14" x 11"



Content

- **Do Not** send any artwork that contains trademarked images or brands such as Disney Characters, Dell, Google, Twitter, etc.
- For additional information on copyright visit: http://www.copyrightkids.org/
- **Do Not** put any identifying information (such as student's full name or age) on the front of the poster.
- Adults may offer minimum technical support but cannot aid in the creative process.
- No professional (paid) assistance is allowed.
- Inappropriate or offensive language and images will cause a submission to be automatically disqualified.

Please Note:

- Students may use a variety of media, such as watercolor, pen and ink, crayon, chalk, or markers.
- Brighter colors will reproduce better when printed.
- Light pencil marks will not show up.
- Keep in mind most posters will likely be on public display, and should be easy to see or read.

Submitting Entries

Kids Safe Online
MS-ISAC® Poster Contest

If Your State is Holding a Contest:

Submit all posters to your state contest (contact contest@cisecurity.org for your state's submission email address). The state will then submit the winning entries to the Multi-State Information Sharing & Analysis Center.

If Your State is Not Holding a Contest:

Each participating school/youth group is permitted to submit up to fifteen (15) posters (5 entries per grade group). How your school/youth group decides on the fifteen (15) posters is up to you! Some schools/youth groups may wish to have a contest and choose the entries; others may just have the art teacher, principal or group leader choose.

Entry Form

Each poster must be accompanied by a completed Entry Form. (See the next page.)

January 2023
Monday 23

Due Date

The posters with the Entry Form, must be submitted electronically by Monday, January 23, 2023. (Limited to one entry per student).

Scanned entries and forms must be electronically submitted to:

contest@cisecurity.org

Notice:

All entries submitted become the property of the Multi-State Information Sharing and Analysis Center and may be used in future publications. Poster entries will not be returned.

Winners

Winners from each grade group (K-5, 6-8, 9-12) will be selected.

A total of 13 winners will have their artwork displayed in our Kids Safe Online Activity Book, which will be distributed throughout the country and used in campaigns to raise awareness among children of all ages about Internet and computer safety. The top four submissions will also be made into posters promoting cybersecurity practices.

The MS-ISAC will notify the school contact person named on the Poster Entry Form or the state contact if their student is a winner!

Questions

Contact the MS-ISAC at:

contest@cisecurity.org

or

call 518 880.0699

CYBERSECURITY AWARENESS MONTH

Kids Safe Online

MS-ISAC® Poster Contest

Entry Form

It is requested that a Teacher or School Contact Person verifies that this form is completely and accurately filled out.

Please attach this form to the corresponding poster in the email. Both the scanned entries and forms must be electronically submitted to: ✉ contest@cisecurity.org

All Fields Are Required

Student's FIRST Name:
(Please DO NOT include
student's last name)

Grade:

Title of Poster:

School Contact Name:

Email:

Phone Number:

School Name:

School Address:

School City:

State:

Zip:

Total Number of
Poster Entries
Judged at School:

MS-ISAC®

Helping Keep Kids Safe Online

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®