

# MAKE A DIFFERENCE IN THE WORLD OF ONLINE SAFETY AND CYBERSECURITY

BECOME A **STOP. THINK. CONNECT.™** PARTNER



STOP | THINK | CONNECT™

# BE A PART OF SOMETHING BIG!

SECURING THE INTERNET IS A RESPONSIBILITY WE ALL SHARE.

STOP. THINK. CONNECT.™ is simple, actionable advice that everyone can follow to stay safer and more secure online.

**STOP.**

make sure  
security  
measures are  
in place.

**THINK.**

about the  
consequences  
of your actions  
and behaviors  
online.

**CONNECT.**

and enjoy the  
Internet.

# STOP. THINK. CONNECT. PARTNERS

HERE'S A SAMPLE OF STOP. THINK. CONNECT.™'S **MORE THAN 630 PARTNERS:**

AT&T  
Comcast  
Facebook  
Google  
Hallmark Cards  
MasterCard

Match.com  
PayPal  
Sony Pictures  
Entertainment  
T-Mobile  
Target

Twitter  
Verizon  
Visa  
Walgreens  
Warner Bros.

See a full list of partners: <https://stopthinkconnect.org/get-involved/our-partners>



STOP | THINK | CONNECT™

# ABOUT US

**STOP. THINK. CONNECT.™** is the global online safety education and awareness campaign to help all digital citizens stay safer and more secure online. The research-based message was created in 2009 by an unprecedented coalition of private companies, nonprofits and government with leadership provided by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). The Department of Homeland Security provides the federal government's leadership for the campaign.





# A PRESIDENTIAL LAUNCH



President Barack Obama declared STOP. THINK. CONNECT.™ the national cybersecurity awareness campaign during his 2010 Presidential Proclamation of National Cyber Security Awareness Month.

*“Together with businesses, community-based organizations and public- and private-sector partners, we are launching a National Cybersecurity Awareness Campaign: ‘STOP. THINK. CONNECT.™’ Through this initiative, Americans can learn about and become more aware of risks in cyberspace, and be empowered to make choices that contribute to our overall security.”*

*– President Barack Obama*



# THE WHITE HOUSE SUPPORTS NEW STOP. THINK. CONNECT.™ EFFORTS

On February 9, 2016, President Obama announced the Cybersecurity National Action Plan (CNAP), highlighting that NCSA will work with industry to launch a National STOP. THINK. CONNECT.™ Cybersecurity Awareness Campaign to empower Americans to secure their online accounts.



## PRESIDENT OBAMA'S ANNOUNCEMENT:

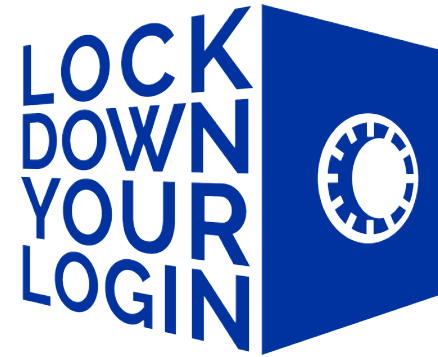
<https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>



STOP | THINK | CONNECT™



STOP | THINK | CONNECT™



As called for in the CNAP, on Sept. 28, 2016, NCSA and more than 40 companies and NGOs announced Lock Down Your Login, a STOP. THINK. CONNECT.™ initiative to encourage a move beyond usernames and passwords to a widespread adoption of strong authentication for key online accounts. The Lock Down Your Login materials, including videos, memes and advice for enabling strong authentication, can be found at [lockdownyourlogin.org](http://lockdownyourlogin.org).





# HOW YOUR COMPANY CAN JOIN THE CAMPAIGN

## REGISTER YOUR ORGANIZATION AND BECOME A STOP. THINK. CONNECT.™ PARTNER.

It's easy and free to sign up for a license. Partners receive access to a wealth of innovative, educational materials that can be personalized, co-branded and used in awareness efforts. You can also create your own resources using STOP. THINK. CONNECT.™ messaging.



### 5 WAYS TO HELP EMPLOYEES BE #PrivacyAware

1. Challenge your employees to think critically about privacy, and make it a fun competition: Ask each employee or department to take the Data Privacy Day theme, "respecting privacy, safeguarding data and enabling trust," and articulate how the theme applies to the work they do on a daily basis, regardless of their department. Brainstorm ideas for operationalizing the Data Privacy Day principles.
2. Foster ongoing learning and engagement: Help employees stay up to date on safe privacy practices at home too by encouraging them to sign up for the National Cyber Security Alliance's (NCSA's) monthly family newsletter, #CyberAware. NCSA does not share our contact lists (period). <http://dprivacyd.info/dpaware>
3. Create a #PrivacyAware culture: Post messages about privacy around the office or on internal message boards or use other available communication platforms now through Jan. 28. To get started, take a look at these posts and memes: [dprivacyd.info/dpaware](http://dprivacyd.info/dpaware)
4. Energize privacy awareness with young people: Teaching about privacy increases one's own privacy awareness. Organize a company-wide volunteer day with local schools to teach students about privacy and online safety. You can use these free teaching materials and lesson plans from C-SAVE: <http://dprivacyd.info/teachprn>
5. Talk to employees frequently about what privacy means to your organization and the role they have in making sure privacy is achieved and maintained. Organize a "lunch & learn" – possibly with outside speakers in January – to educate employees about the value and impact of protecting customer and colleague information and their role in keeping it safe. Videos and other resources to help you start the conversation can be found here: [dprivacyd.info/privlibrary](http://dprivacyd.info/privlibrary)



### Do a Digital Spring Cleaning and Clear Out Cyber Clutter

A few simple steps will help you stay cyber safe and protect your personal data and identity all year round.

The National Cyber Security Alliance (NCSA) and Better Business Bureau (BBB) are encouraging consumers to get their online lives in good order by conducting a thorough cleanse of their cyber clutter. With preventing identity theft a top safety concern for Americans,<sup>1</sup> NCSA and BBB urge everyone to make "digital spring cleaning" an annual ritual to help protect valuable personal data.

**REFRESHING YOUR ONLINE LIFE IS A RELATIVELY SIMPLE PROCESS. NCSA HAS IDENTIFIED THE TOP TROUBLE-FREE TIPS EVERYONE SHOULD FOLLOW THIS SPRING.**

**KEEP A CLEAN MACHINE:** Ensure all software on internet-connected devices – including PCs, smartphones and tablets – is up to date to reduce risk of infection from malware.

**LOCK DOWN YOUR LOGIN:** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Begin your spring cleaning by fortifying your online accounts and enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device.

**DECLUTTER YOUR MOBILE LIFE:** Most of us have apps we no longer use and some that need updating. Delete unused apps and keep others current, including the operating system on your mobile device.

**DO A DIGITAL FILE PURGE:** Perform a good, thorough review of your online files. Tend to digital records, PCs, phones and any device with storage just as you do for paper files. Get started by doing the following:

- o Clean up your email: Save only those emails you really need and unsubscribe to email you no longer need/want to receive.
- o Back up your files: Important data has a way of disappearing. Back up your files to a secure location, such as a cloud storage service or an external hard drive.



### SIMPLE CYBERSECURITY TIPS FOR STAYING SAFE ONLINE DURING TAX TIME

Tuesday, April 18 might feel far-off, but the tax filing deadline will be here before you know it. That also means it's prime time for cyber thieves and their devious online scams. Tax identity theft – which occurs when someone uses your Social Security number to file a tax return and then steals your refund – is on the rise. According to the Federal Trade Commission (FTC), there was a nearly 50 percent increase in identity theft complaints in 2015, and by far the biggest contributor to the surge was the spike in tax refund fraud.<sup>1</sup> At this time last year, the Internal Revenue Service (IRS) reported a 400 percent increase in email phishing and malware incidents aimed at both taxpayers and tax professionals.<sup>2</sup> Cyber crooks are crafty: they can break into your account or device and literally steal your digital life – and your money. The National Cyber Security Alliance (NCSA) and Identity Theft Resource Center (ITRC) have teamed up to share cautionary tips for spotting cyber tricks, proactive online safety steps and invaluable advice about how to get help if you fall victim to tax identity theft.

**DON'T BECOME A VICTIM: WATCH OUT FOR TAX SEASON TRICKS**

Online outlaws will attempt to lure you in a variety of ways. Watch out for the following:

- **Fraudulent tax returns:** The FTC recommends trying to file your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If the file is yours and it's in early, it makes it impossible for a cyber thief to submit another return with your personal information. It's also important to always use smart practices with your personal information. Remember to only share your Social Security number when it's absolutely necessary. Check your credit report regularly for shady activity and never throw papers with critical information – like your Social Security number or bank account information – in the trash. It's best to shred all paper containing personal data.<sup>3</sup>
- **Phishing and malware:** Cybercriminals will try to get you to do "something" so they can steal your personal information. Watch out for unsolicited emails, texts, social media posts or fake websites that may prompt you to click on a link or to share valuable personal and financial information. Armed with this information, online thieves can pilfer funds and/or commit identity theft. And unfamiliar links or attachments can contain malware – viruses, spyware and other unwanted software that gets installed on your computer or mobile device without your consent – which can infect your computer files if opened.





# WHAT STOP. THINK. CONNECT.™ PARTNERS RECEIVE

A partner toolkit to help you get started

Access to the Partner Resource Center, which houses STOP. THINK. CONNECT.™ branding, logos, templates and more

A monthly partner newsletter

Ongoing opportunities to get involved with NCSA and STOP. THINK. CONNECT.™



Dear STOP. THINK. CONNECT. partner,  
Here's what we've been up to lately:

## Welcome

We would like to welcome the following recently added partners: 88innovations Limited; Ameri-X-Guard Inc.; Authority of the Tennessee Attorney General; Barclays; Black River Technologies LLC; Brookfield Renewable; Cisco; Comprehensive Financial Services, LLC; Cone Health; Emporia State University; Integrity Technology Solutions; LP3-SecurIT; Mike the Tech Guy; Santa Cruz Public Libraries; SSI GUARDIAN, LLC; Staples; Supportdesk; Upgraded Era; VMware; and WINS1, LLC.

Partners also receive creative license to use STOP. THINK. CONNECT.™ branding and messaging for online safety awareness efforts. We have some great samples to share...



STOP | THINK | CONNECT™

# SAMPLE OF NCSA-CREATED RESOURCES

## NAVIGATING YOUR CONTINUOUSLY CONNECTED LIFE

Every day, we connect to the internet in ways you may not even realize. The Internet of Things (IoT) is like an "Internet of Me": it connects everything and everyone, including your home, the businesses you use, and the larger digital community, and uses your data to help you manage your life.

88 PERCENT of Americans have a smart home device (and that number is growing).

DATA PRIVACY DAY



### 5 WAYS TO HELP EMPLOYEES BE PrivacyAware

1. Challenge your employees to think critically about privacy, and make it a fun competition: Ask each employee or department to take the Data Privacy Day theme, "respecting privacy, safeguarding data, enabling trust," and articulate how the theme applies to the work they do on a daily basis, regardless of their department. Brainstorm ideas for operationalizing the Data Privacy Day principles.
2. Foster ongoing learning and engagement: Help employees stay up to date on safe privacy practices. Sign up for the National Cyber Security Alliance's (NCSA's) monthly family newsletter, #CyberAware. NCSA does not share our contact lists (period). <http://dprivacyd.info/dpoboxes>
3. Create a #PrivacyAware culture: Post messages about privacy around the office or on internal message boards or use other available communication platforms now through Jan. 28. To get started, take a look at these posts and memes: [dprivacyd.info/1c8Fqj7](http://dprivacyd.info/1c8Fqj7).
4. Energize privacy awareness with young people: Teaching about privacy increases one's own privacy awareness. Organize a company-wide volunteer day with local schools to teach students about privacy and online safety. You can use these free teaching materials and lesson plans from C-SAVE: <http://dprivacyd.info/teachpage>.
5. Talk to employees frequently about what privacy means to your organization and the role they have in making sure privacy is achieved and maintained. Organize a "lunch & learn" – possibly with outside speakers in January – to educate employees about the value and impact of protecting customer and colleague information and their role in keeping it safe. Videos and other resources to help you start your conversation can be found here: [dprivacyd.info/privlibrary](http://dprivacyd.info/privlibrary).

## Do a Digital Spring Cleaning and Clear Out Cyber Clutter

A few simple steps will help you stay cyber safe and protect your personal data and identity all year round.

The National Cyber Security Alliance (NCSA) and Better Business Bureau (BBB) are encouraging consumers to get their online lives in good order by conducting a thorough cleanse of their cyber clutter. With preventing identity theft a top safety concern for Americans,<sup>1</sup> NCSA and BBB urge everyone to make "digital spring cleaning" an annual ritual to help protect valuable personal data.

REFRESHING YOUR ONLINE LIFE IS A RELATIVELY SIMPLE PROCESS. NCSA HAS IDENTIFIED THE TOP TROUBLE-FREE TIPS EVERYONE SHOULD FOLLOW THIS SPRING.

**KEEP A CLEAN MACHINE:** Ensure all software on internet-connected devices – including PCs, smartphones and tablets – is up to date to reduce risk of infection from malware.

**LOCK DOWN YOUR LOGIN:** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Begin your spring cleaning by fortifying your online accounts and enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device.

**DECLUTTER YOUR MOBILE LIFE:** Most of us have apps we no longer use and some that need updating. Delete unused apps and keep others current, including the operating system on your mobile device.

**DO A DIGITAL FILE PURGE:** Perform a good, thorough review of your online files. Tend to digital records, PCs, phones and any device with storage just as you do for paper files. Get started by doing the following:

- o Clean up your email: Save only those emails you really need and unsubscribe to email you no longer need/want to receive.

o Back it up: Copy important data to a secure cloud site or another computer/drive where



JANUARY 28, 2017



PrivacyAware

## DATA PRIVACY DAY

is an international effort, held annually on Jan. 28, to empower individuals and businesses to respect privacy, safeguard data and enable trust.



## SIMPLE CYBERSECURITY TIPS FOR STAYING SAFE ONLINE DURING TAX TIME

Wednesday, April 18 might feel far-off, but the tax filing deadline will be here before you know it. That also means it's primetime for cyber thieves and their devious online scams. Tax identity theft – which occurs when someone uses your Social Security number to file a tax return and then steals your refund – is on the rise. According to the Federal Trade Commission (FTC), there was a nearly 50 percent increase in identity theft complaints in 2015, and by far the biggest contributor to the surge was the spike in tax refund fraud.<sup>1</sup> At this time last year, the Internal Revenue Service (IRS) reported a 400 percent increase in email phishing and malware incidents aimed at both taxpayers and tax professionals.<sup>2</sup> Cyber crooks are crafty: they can break into your account or device and literally steal your digital life – and your money. The National Cyber Security Alliance (NCSA) and Identity Theft Resource Center (ITRC) have teamed up to share cautionary tips for spotting cyber tricks, proactive online safety steps and valuable advice about how to get help if you fall victim to tax identity theft.

### DON'T BECOME A VICTIM: WATCH OUT FOR TAX SEASON TRICKS

Online outlaws will attempt to lure you in a variety of ways. Watch out for the following:

- **Fraudulent tax returns:** The FTC recommends trying to file your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If the file is yours and it's in early, it makes it impossible for a cyber thief to submit another return with your personal information. It's also important to always use smart practices with your personal information. Remember to only share your Social Security number when it's absolutely necessary. Check your credit report regularly for shady activity and never throw papers with critical information – like your Social Security number or bank account information – in the trash. It's best to shred all paper containing personal data.<sup>3</sup>
- **Phishing and malware:** Cybercriminals will try to get you to do "something" so they can steal your personal information. Watch out for unsolicited emails, texts, social media posts or fake websites that may prompt you to click on a link or to share valuable personal and financial information. Armed with this information, online thieves can pilfer funds and/or commit identity theft. And unfamiliar links or attachments can contain malware – viruses, spyware and other unwanted software that gets installed on your computer or mobile device without your consent – which can infect your computer files if opened.



STOP | THINK | CONNECT™



# STOP. THINK. CONNECT.™ AROUND THE WORLD



## ENISA/EUROPEAN CYBER SECURITY MONTH



## CIBERVOLUNTARIOS



## PUBLIC SAFETY CANADA



## COUNCIL OF ANTI-PHISHING JAPAN



# SAMPLE OF PARTNER-CREATED RESOURCES

## ESET/NCSA



**BEHIND OUR DIGITAL DOORS: CYBERSECURITY & THE CONNECTED HOME**

**Executive Summary**

In support of National Cyber Security Awareness Month (October), ESET® and the National Cyber Security Alliance (NCSA) commissioned a survey to better understand the role of cybersecurity in the American household, providing an inside-look into how it is adapting in the digital era of the data breach. Given the simultaneous rise in our number of connected devices and cyber threats, this survey underlined the importance of cybersecurity as a core commitment in our digital lives.

## FEDERAL TRADE COMMISSION



**OnGuardOnline.gov**

STOP | THINK | CONNECT

Vea esta página en español

**Just for You Parents**

Kids spend time online: chatting with friends, sharing photos, doing homework. The internet offers a world of opportunities, but there are risks, too.

The best way to protect your kids online? Talk to them. Kids rely on their parents for important information – like how to be safe and responsible online.

## HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY (HIMSS)



**THE 2015 HEALTHCARE ORGANIZATION'S GUIDE TO KEEPING INFORMATION SAFE AND SECURE**

Why industry-wide defensive measures are on the rise

Results from the 2015 HIMSS Cybersecurity Survey:

**68%** of respondents' organizations experienced a significant security incident.

## U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)



**SHARING ONLINE IS SERIOUS BUSINESS**

Homeland Security

STOP | THINK | CONNECT

## PRIVATE WIFI



On-the-Go WiFi Safety

**5 ONLINE SECURITY TIPS FOR SMARTER TRAVEL**

Don't let online security concerns derail your travel plans.

Whether you plan to explore the US on a road trip, hit the beach in the Caribbean, tour a castle in Europe, or hike in South America, these five WiFi safety tips will keep you secure throughout your journey.

**1 Keep a clean machine.**  
Ensure your devices are up-to-date with the latest antivirus, firewall protection and operating system patches.

**2 Stop and think before you connect to public WiFi.**  
WiFi is available everywhere you go, including in airports, hotels, restaurants, parks, and museums, but these networks are completely open and insecure. Use common sense when you connect to public WiFi and be cautious about the when you click and the information you send.

**3 Paid WiFi doesn't mean safe WiFi.**  
Just because you paid for WiFi access, it doesn't mean it's safe. There is no exception to stop anyone from eavesdropping on your communications, so make sure you protect yourself from hackers.

**4 Beware of evil twins.**  
Hackers sometimes set up evil twins – WiFi networks that look real – near legitimate public WiFi networks. If you connect to them, all of your communications can be captured. It can be hard to tell the difference so confirm the name of the hotspot with the owner before you connect.

**5 Use a VPN to encrypt information on all of your devices.**  
If you use public WiFi while you travel, the only way to guarantee your security is to use a virtual private network (VPN) like PRIVATE WiFi to encrypt your personal data in wireless hotspots. Remember, WiFi signals are just radio waves. Anyone in range can "listen in" to what you send and receive. Antivirus or firewall software won't protect you – but a VPN encrypts all of your communications no matter where your travels take you.

Private WiFi

STOP | THINK | CONNECT

# PARTNER-CREATED RESOURCES

(CONTINUED)

MATCH.COM

The screenshot shows the Match.com homepage with a navigation bar at the top. The main content area is titled "Good Advice - Safety Tips to Follow". It includes a sub-header "Online Safety Tips" and several sections of advice: "Protect your finances", "Guard your personal and online access information", and "Be Web Wise". A small graphic of a person sitting at a desk is visible on the right side of the page.

MICROSOFT

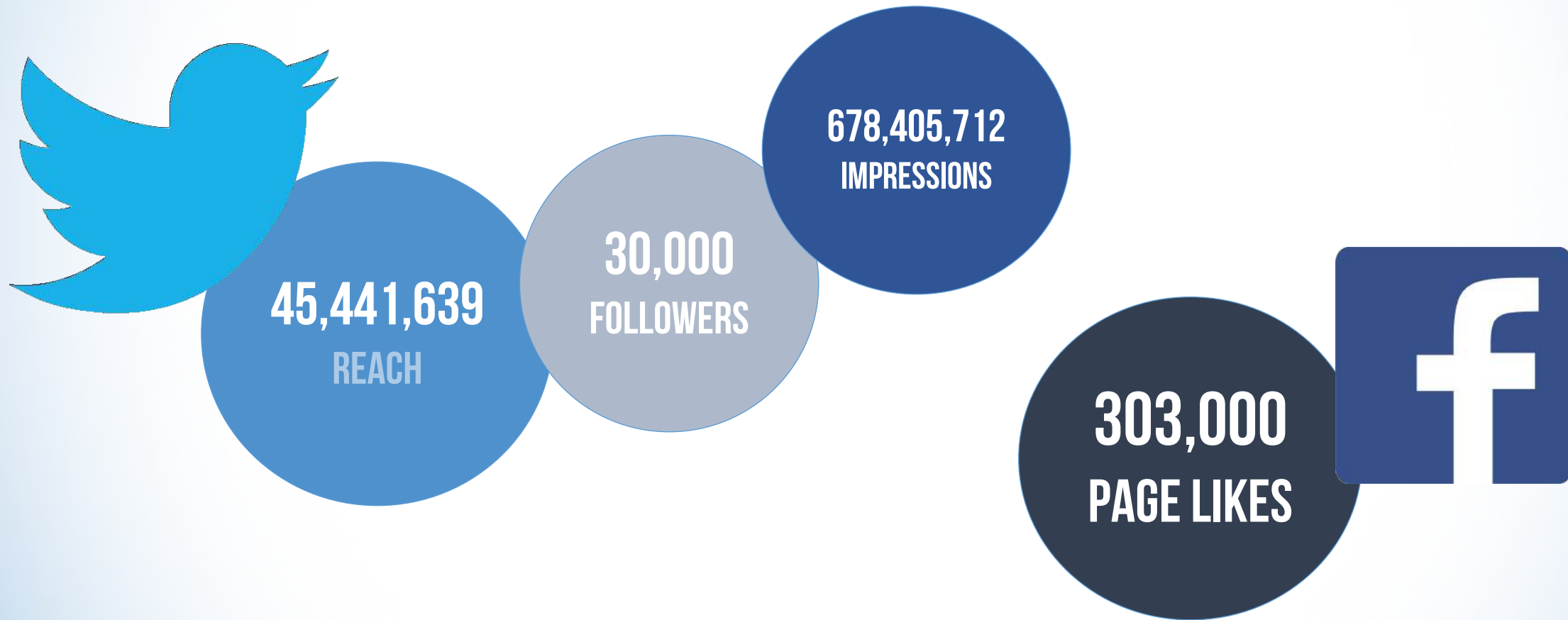
The screenshot shows the Microsoft Safety & Security Center page. The main heading is "Online bullying: identifying target, bully, and bystander behavior". Below this, there is a section titled "You have the power to help Stop Online Bullying" with a "Take the quiz" button. To the right, there is a sidebar with "I want to..." options and "Related links". The page is designed with a clean, professional layout using Microsoft's branding.

GOOGLE

The screenshot shows the Google "Good to Know" page. The heading is "Good to Know" with the subtitle "How to be safe on the Internet and manage the information you share online". The page features a large illustration of a person being attacked by a robot, with a bear and a person holding a shield nearby. At the bottom, there is a "STOP | THINK | CONNECT" logo and a link to "www.google.com/goodtoknow".

# STOP. THINK. CONNECT.™ ON SOCIAL MEDIA

AS OF APRIL 2017







STOP | THINK  
CONNECT™

600  
PARTNERS  
91% PARTNER GROWTH

IN

50+  
COUNTRIES

72%  
OF TEENS

RECOGNIZE  
STOP. THINK. CONNECT.™  
ADVICE

Keep a Clean Machine  
Own Your Online Presence  
Lock Down Your Login  
Share With Care



ChatSTC

16  
TWITTER  
CHATS

25  
MILLION  
POTENTIAL  
REACH

488  
MILLION  
POTENTIAL  
IMPRESSIONS

# STOP. THINK. CONNECT.™ ACCOMPLISHMENTS

In the last year<sup>1</sup>, the STOP. THINK. CONNECT.™ campaign generated

**486,058,605 IMPRESSIONS**

in a variety of consumer, political, business and trade outlets across all forms of media including print, online print and broadcast.

**The Mercury News**



THE  
HUFFINGTON  
POST

**POLITICO**  
**Bloomberg**



STOP. THINK. CONNECT.™ Tips have been  
**TRANSLATED INTO FIVE LANGUAGES.**

**MORE THAN 100 ONLINE SAFETY RESOURCES**

are available on [stopthinkconnect.org](http://stopthinkconnect.org).

# MORE INFORMATION

ADDITIONAL DETAILS ABOUT BECOMING A PARTNER CAN BE FOUND AT

**[HTTPS://STOPTHINKCONNECT.ORG/GET-INVOLVED](https://stopthinkconnect.org/get-involved)**

CONTACT US AT

**[INFO@STOPTHINKCONNECT.ORG](mailto:info@stopthinkconnect.org)**



STOP | THINK | CONNECT™