



Resources for an Innovative Awareness Program

Thursday, June 24, 2019
FISSEA Conference
Gaithersburg, Maryland

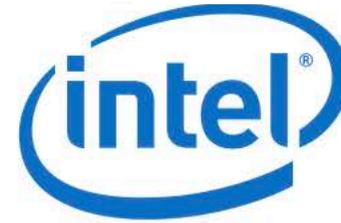
About NCSA

Established in 2001 by industry and government.

Works closely with the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA) and other agencies.

26 board industry members.

Thousands of partners from industry, government and nonprofits.



NATIONAL CYBERSECURITY ALLIANCE

NCSA Board Members

NCSA's mission is to educate and empower our global digital society to use the internet safely and securely. Our core strengths are:



EDUCATE



AMPLIFY



CONVENE

StaySafeOnline.org

Core Programs



National Cybersecurity
Awareness Month



STOP | THINK | CONNECT™

Helpful Content You Can Expect

Campaign
Toolkits to
help you get
started

Campaign logos and
template emails to
employees.

Webinars and
videos

Online library with
social graphics,
fact sheets,
research and tip
sheets.

Content from
government,
industry and
nonprofits

SAMPLE OF NCSA-CREATED RESOURCES



NATIONAL CYBERSECURITY ALLIANCE DATA PRIVACY DAY

ARE YOU DOING ENOUGH TO PROTECT CONSUMERS' DATA

Nearly 75 percent of Americans feel it is "extremely" or "very" important that companies have "easy-to-understand, accessible information about what personal data is collected about them, how it is used and with whom it is shared."

PERSONAL INFORMATION MAY BE VALUABLE TO YOUR BUSINESS BUT IT'S ALSO SOMETHING CONSUMERS VALUE.
Together we can create a culture of respecting privacy, safeguarding data and

HOW TO MANAGE YOUR PRIVACY IN A GROWING INTERNET OF ME

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT. Be thoughtful about how your personal information is collected through apps and websites. This information can often be found in a company's privacy policy.

OWN YOUR ONLINE PRESENCE Set the privacy and security settings on at least one service and/or device to your comfort level for information sharing.

LOCK DOWN YOUR LOGIN Choose one account and turn on the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

LOCK DOWN YOUR LOGIN

STOP | THINK | CONNECT **ITRC** IDENTITY THEFT RESOURCE CENTER

STAY SAFE FROM CYBERCRIME DURING TAX TIME

favorite time of year – tax season – is creeping up on the calendar. Tuesday, April 17, may feel like the filing deadline will be here before you know it. Tax season is primetime for online scams. According to the Federal Trade Commission (FTC), tax-related identity theft – when a criminal uses a victim's Social Security number along with other personal data to file an income tax return (and reap the rewards) – is the most common type of identity theft. In fact, a 2017 Identity Fraud Study by Javelin Strategy & Research revealed that nearly one in three consumers notified that their data has been breached during tax season. With the recent Equifax cyberattack still fresh in our minds, more than 145 million Americans' names, addresses, birthdates, Social Security numbers and other sensitive information are at risk. Cybercriminals are crafty and continuously looking for ways to steal your personal information. The Internal Revenue Service (IRS) indicates that phishing schemes continue to lead its "dirty dozen" list of tax scams. So what is the average American to do? The National Cyber Security Alliance (NCSA) and the Identity Theft Resource Center (ITRC) have once again joined forces to help consumers keep safe during tax season. Here are some tips for identifying cyber scams, actionable online safety steps and what to do if you fall victim to identity theft.

TARGETING TAXPAYERS
There has been a surge in cybercriminal swindles directed at consumers. If you protect yourself against these phishing schemes, your identity and tax return will be safer and more secure.

PERSONATION PHONE SCAMS
Phishing attempts to be IRS employees – using fake names and phony IRS ID numbers – may ring you and insist on your money and it must be paid as soon as possible through a gift card or wire service. If the call is not legitimate, the scammers often leave an emergency callback request message. The real IRS will not call you and demand immediate payment; in general, it will mail you a bill if you owe money.

INCREASE IN PHISHING, EMAIL AND MALWARE SCHEMES



Sneak Peak: Topics for NCSAM

- Weekly cyber safe habits related to top threats – phishing, public WIFI, updates and more.
- Personal accountability
- Proactive behavior
- Consumer connected devices
- Privacy
- Ecommerce security



National Cybersecurity
Awareness Month

Get Access and Get Involved

1. Sign up for NSCA's email list
<https://staysafeonline.org/email-signup/>
2. Sign up as a NCSAM Champion
<https://staysafeonline.org/ncsam/>
3. Stay in touch and share your ideas