A voice for cybercrime victims

Kristin Judge
CEO/President
Guiding Principles

(1) bringing a voice to and serving the victims of cybercrime;
(2) ensuring victims are connected to local, state and federal law enforcement when needed;
(3) working within existing law enforcement and victim assistance systems to enhance service, collaboration and reporting;
(4) providing effective training based on adult learning principles; and
(5) promoting education and awareness for all citizens.
THE PROBLEM

As incidences of cybercrime continue to grow, victims are searching for direction and resources.

Currently, victims struggle to find the right help, and responses from law enforcement vary by jurisdiction.

301,580

victims reported to FBI/IC3 in 2017

1.4 billion

victim losses reported to FBI/IC3 in 2017

THE SOLUTION

CSN is bringing together partners around the country to create a coordinated system to support cybercrime victims.

Soon, the victims will have one number to call and reach a referral specialist who can navigate them through the process of response and recovery.

15%

estimated number of victims who report cybercrime to FBI/IC3

CYBERCRIMESUPPORT.ORG
FraudSupport.Org – Mid-October

Fraud Can Happen to Anyone

I need help with...

- Identity Theft
- Text/email spam or phish
- Goods/Services
- Computer Intrusion (malware)
- Fraud (Financial)
- Business Hacked
- Harassment/Threats/Stalking
- Ransomware
- Scams and Impersonation
- Wired money to scammer

SEE ALL CATEGORIES
National Cybersecurity Awareness Month

BE A PART OF SOMETHING BIG
GET INVOLVED ON SOCIAL MEDIA

Use #CyberAware on Twitter
Like StaySafeOnline on Facebook
Follow @StaySafeOnline on Twitter

JOIN THE #CHATSTC TWITTER CHATS EVERY THURSDAY IN OCTOBER AT 3 P.M. EDT/NOON PDT

STAYSAFEONLINE.ORG/NCSAM
Contact NCSA

info@staysafeonline.org

STAYSAFEONLINE.ORG

SIGN UP FOR OUR MAILING LIST TO RECEIVE THE LATEST NCSAM NEWS AND CONTENT
STAYSAFEONLINE.ORG/ABOUT-US/CONTACT-US
What is Cybersecurity?

Take out a piece of paper and pen....
5 Steps to a Safer Online Life

1. **Identify** important devices, data and accounts
2. **Protect** your online life
3. **Detect** when something goes wrong
4. **Respond** quickly and fix the issue
5. **Recover** from a loss
Step 1. **Identify** important devices, data and accounts

What are the most sensitive/important devices, data and accounts you have?
<table>
<thead>
<tr>
<th>Phone</th>
<th>Photos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tablet</td>
<td>Facebook</td>
</tr>
<tr>
<td>Exercise Tracker</td>
<td>Twitter</td>
</tr>
<tr>
<td>Home Security</td>
<td>Instagram</td>
</tr>
<tr>
<td>Television</td>
<td>SnapChat</td>
</tr>
<tr>
<td>Virtual Assistants</td>
<td>WhatsApp</td>
</tr>
</tbody>
</table>
Step 2. **Protect** your online life

What are you doing to protect your digital life currently?
Passwords
Two-Factor Authentication
Privacy Settings

VPN (Virtual Private Network)
Back Up
Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.

Add your own favorite site by submitting a pull request on the GitHub repo.

Search websites

Backup and Sync
Banking
Cloud Computing
Communication
Cryptocurrencies

Developer
Domains
Education
Email
Entertainment
<table>
<thead>
<tr>
<th>Social Media Platform</th>
<th>✅</th>
<th>✔️</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pinterest</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Plurk</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Quora</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Reddit</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Snapchat</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Stack Exchange</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Tumblr</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Twitter</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>VanillaForums.com</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>Viadeo</td>
<td>✅</td>
<td>✔️</td>
</tr>
<tr>
<td>VK</td>
<td>✅</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Follow these six simple steps to gain peace of mind and more control over your online security.

Compromised accounts cause reputational harm and embarrassment and put others at risk through the spread of malware and viruses. You have enough to worry about, so what can you do about it?
6 Steps to Better Security

- Protect accounts with strong authentication
- Keep software updated
- Avoid phishing attempts
- Use unique passwords
- Protect mobile devices
- Use trusted security tools

www.LockDownYourLogin.org
Step 3. **Detect** when something goes wrong

If someone compromised/hacked your devices or accounts, how would you know?
Device Keeps Running

Pop-Up Ads

Anti-Virus

Unwanted Updates or Tools Show Up

Friends Get Requests
Step 4. **Respond** quickly and fix the issue

How would you respond if your devices, data or accounts were hacked?
Find a Professional
IdentityTheft.gov
Update and Check Apps
FTC.Gov
Reset Settings
Step 5. **Recover** from a loss

What will it take to recover after having your data or devices hacked?
Protect Your Money

Investor protection is an integral part of FINRA’s mission. Unfortunately, far too many investors fall victim to Ponzi schemes, pump-and-dump scams and other types of investment fraud. The good news is that fraud and the growing threat of identity theft can often be avoided.

We’ll help you spot the red flags of fraud and identity theft, and avoid the persuasion tactics of fraudsters. It’s also vital to know the right questions to ask about investments and the people who pitch them—and where to go to verify the answers. After all, it’s your money—learn how to protect it.

Investor Alerts
Check out the latest Investor Alerts from FINRA and other regulators.

Avoid Fraud
Even if you have never been subjected to an investment fraudster’s sales pitch, you probably know someone who has. The more you know about the types of fraud and tactics used the better equipped you’ll be to avoid it.

Ask and Check
Ask the right questions and verify the answers before you work with an investment professional or buy an investment product.

Protect Your Identity
Identity theft occurs when someone obtains your personal information and uses it to steal your money or commit fraud or other crimes. Here’s how to safeguard your identity.
Report identity theft and get a recovery plan

Get Started

or browse recovery steps

IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:

Tell us what happened.
We'll ask some questions about your situation. Tell us as much as you can.

Get a recovery plan.
We'll use that info to create a personal recovery plan.

Put your plan into action.
If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
When things just don't add up...

CALL FOR HELP

LIVE CHAT

BLOG
BREACHES
SCAMS
SUPPORT US

https://www.idtheftcenter.org
App Safety Center

Tips, information, and considerations for the safe development and use of smartphone apps.

SAFETY CHECK

If you think someone is monitoring your device, visit this website from a computer, tablet, or smartphone that isn’t being monitored. Exit from this website and delete it from your browser history. For more information, visit this page.

TECHSAFETY.ORG

Managed by the Safety Net Project at the National Network to End Domestic Violence (NNEDV), this blog discusses technology, privacy, and safety in the context of intimate partner violence, sexual assault, and violence against women.

CONTACT US

Search

CATEGORIES

Current Events
Data & Statistics
Feminism & Technology
Safety Net News
Event
Training
Resources

POSTS BY TAG

There’s an app for everything, right? An increasing number of apps for smartphones and tablets are attempting to address the issues of domestic violence, sexual assault, and/or stalking. Some apps are screening tools for survivors and professionals to recognize abuse and find resources. Other apps are meant to be a tool to contact help during an emergency.

With so many apps, knowing which ones to use can be difficult. In addition, as with any technology, when apps are being developed and used by survivors of abuse, there are several things to consider that should be taken to ensure safety, privacy, and accuracy for the user.

The App Safety Center will highlight some of these apps by providing information on what survivors and professionals need to know to use them safely.

Apps & Resources for Survivors

This section includes information on safety and privacy for survivors who may want to use apps, as well as details about several apps currently on the market.

- Choosing and Using Apps: Considerations for Survivors
- Types of Available Apps:
  - Screening and Assessing for Abuse & Safety
  - Safety Apps: Getting Help During an Emergency
  - Apps for Teens & College Students
  - Other Apps for Survivors

Apps for the Public - Awareness & Education

Below are examples of available apps that are meant to inform and engage individuals and communities on domestic violence, sexual assault, and stalking.

- Considerations for Choosing and Using Awareness Apps
- Available Apps:
Consumer.ftc.gov
5 Steps to a Safer Online Life

1. **Identify** important devices, data and accounts
2. **Protect** your online life
3. **Detect** when something goes wrong
4. **Respond** quickly and fix the issue
5. **Recover** from a loss
Continuous Education Is Key!

Resources are Available!