



Cybercrime
SUPPORT NETWORK

Cybercrime Support Network (CSN) is a national nonprofit whose mission is to serve individuals and small businesses impacted by cybercrime.



Recognize.

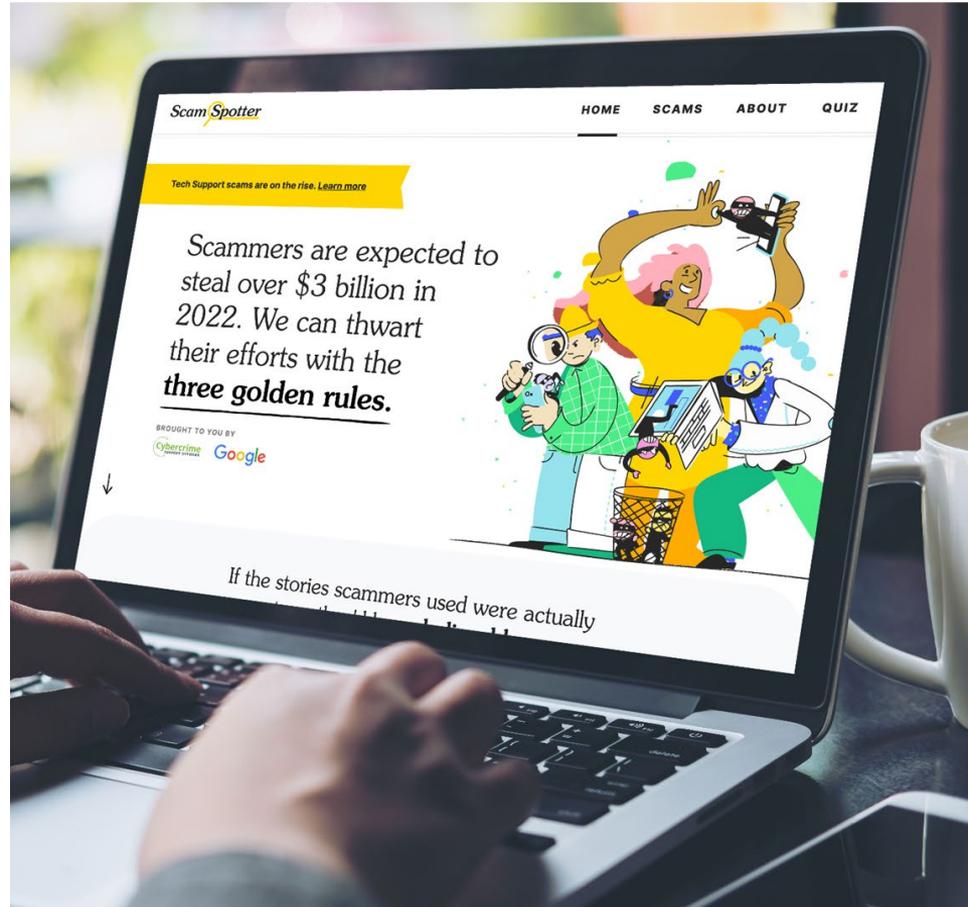
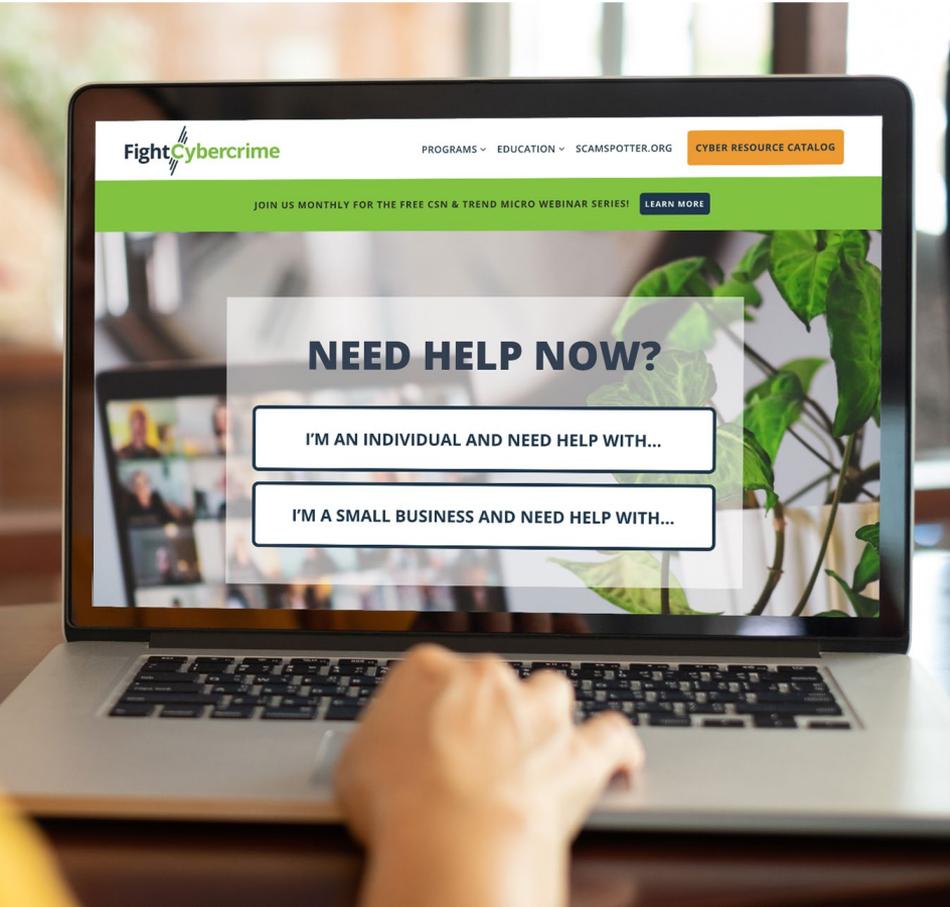


Report.

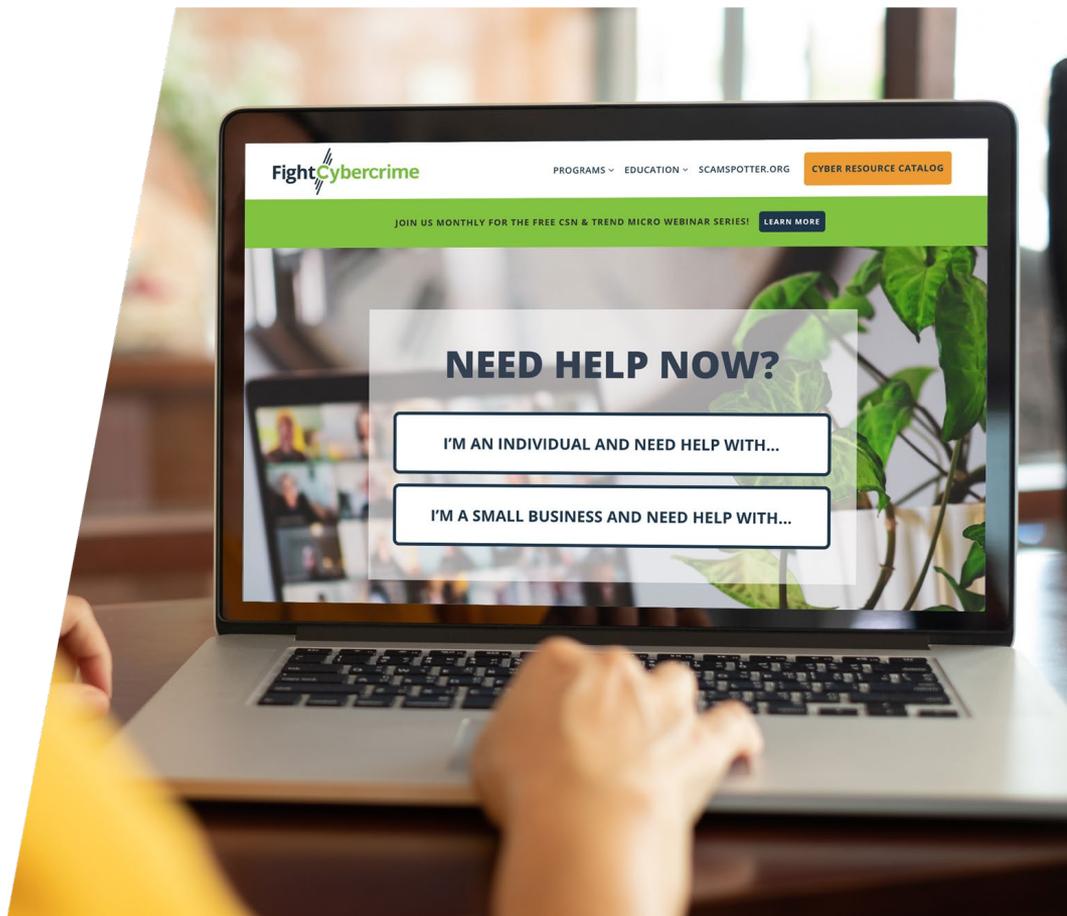


Recover.

Websites



- Resources for individuals and small businesses
- Searchable by crime type
- Guides visitors through the **recognize, report, and recover** process



Cyber Resource Catalog



- Searchable by threat, audience, and keywords
- Vetted resources from CSN and other reputable organizations

CSN Outreach Materials



Is That Text Message Real or Fake?

Cybercriminals send text messages posing as somebody you trust, such as government officials, friends, family, and others, with the goal to steal your money or personal information.

Their common tactics include:

- Threatening you unless you pay a fee or fine
- Offering a great product, service, or investment at a great price
- Asking for you to log in to an account
- Pretending they are friends or family and urgently need money because of some dire event, like getting arrested, hurt, or their money stolen

In general, just delete an unusual or



STEP 1

Determine if it is a reasonable request.

Do you live in the state they are referring to? Would the government contact you via text message? Were you expecting this message?

If not, the text is likely fake.

Determination: B

FightCybercrime.org

EASY E-CLEANUP CHECKLIST

If you find a compromised account during your digital cleanup, visit [FightCybercrime.org](https://fightcybercrime.org).



TIDY UP YOUR DEVICES

Keep all web-connected devices updated and clean.

- UPDATE SOFTWARE**
Minimize exposure to security risks and ensure that your device is performing at optimum speed.
- BRING IN BACKUP**
Back-up valuable files to a secure hard drive or storage cloud.
- CLEAN UP APPS**
Get rid of apps you don't use. For apps you do use, update permissions to control which apps have access to your location, photos, contacts, etc.



REINFORCE YOUR SECURITY

Secure your online accounts to improve your safety online.

- CREATE STRONG PASSWORDS**
Visit www.ConnectSafety.org for tips to create and manage strong passwords.
- ENABLE TWO FACTOR AUTHENTICATION**
Two factor authentication (2FA) requires an additional code to log in.
- ADJUST PRIVACY SETTINGS ON SOCIAL MEDIA**
Go to www.StateSafeCollaborative.org for quick links to update your privacy settings.
- PASSWORD-PROTECT YOUR DEVICES**
Be sure that your laptop, smartphone, and other electronic devices are protected with strong passwords.
- CONSIDER A VPN**
Using a Virtual Private Network offers you a secure, untraceable connection.



REMOVE DIGITAL EXCESS

Get rid of unwanted subscriptions and files.

- UNSUBSCRIBE FROM UNWANTED NEWSLETTERS**
Unsubscribe from automated emails that you no longer need.
- DELETE OLD FILES & APPS**
Sort through your files and apps, and figure out which ones you can get rid of.
- CHECK FRIENDS & FOLLOWERS**
Review your friends lists on social networks and delete anyone who doesn't belong.
- CLEAN UP BROWSER SETTINGS**
Clear out old data, like stored passwords and old autofill information, and set your browser so it doesn't store passwords or financial information.

FightCybercrime.org



CybercrimeSupport.org | FightCybercrime.org | ScanTeam.org
© 2021 Cybercrime Support Network

FIVE STEPS TO COPE WITH CYBERCRIME

Experiencing cybercrime can be as emotionally and mentally draining as any other crime. As a survivor of cybercrime, it is important that you take care of yourself throughout the process of reporting and recovery.

1



TAKE ACTION
Report the cybercrime by reporting, you take the situation from them and you help prevent happening to

3



SEEK SUPPORT
Talk to a trusted friend, member, or a professional

5



CONTACT AN ASSISTANCE
Groups like NCVC are available to assist with recovery you

If you need help, visit [FightCybercrime.org](https://fightcybercrime.org) for more recovery resources.

FightCybercrime.org

WAS YOUR BUSINESS PHISHED?



What is phishing?

Hackers will send emails disguised as a trusted person or company to your employees. The email might include a link to a scam website that will ask them to input their password or username, allowing the hacker access to your data. The phishing email could also include attachments that, when clicked, install malicious software onto your business network.

If you or an employee clicked on a phishing email, don't panic!

Follow these immediate action steps



Disconnect the computer or device from the internet/network.



Send a company-wide email notifying employees of the phishing attack.



Run a virus scan on all computers and devices connected to your business network.



Change any compromised passwords right away and enable two factor authentication (2FA) on all of your accounts - which requires an additional code to log in.



Forward phishing emails or websites to the Anti-Phishing Working Group at reportphishing@apwg.org.



If you think a scammer obtained sensitive information, visit identitytheft.gov for resources to minimize your business's risk of identity theft.

Cyber Tip

Create a workplace culture where employees don't fear discipline if they accidentally click on a phishing email. Employees should feel comfortable telling management right away. Remember, cybercrime and online fraud can happen to anyone, so use this as an opportunity for you and your employees to learn.

Visit [FightCybercrime.org](https://fightcybercrime.org) for more recovery resources.

FightCybercrime.org



CybercrimeSupport.org | FightCybercrime.org | ScanTeam.org
© 2021 Cybercrime Support Network

BUSINESS EMAIL COMPROMISE

New Message

Subject: **WAS YOUR BUSINESS AFFECTED BY BEC?**

Business email compromise (BEC) is a sophisticated scam carried out by fraudsters who compromise email accounts through social engineering or computer intrusion techniques and ask for fraudulent wire account transfers.

Some immediate action steps to take:

- If funds were to be discovered
- Request that you be notified where the fraud occurred
- Alert all employees
- Contact your lawyer
- Change passwords
- Contact your business

BUSINESS MALWARE 101

understanding malware & how to respond if your business is affected



What is malware?

Malware is any type of malicious software, installed without consent, designed to do damage or disable your business's computer system(s) or network.

TYPES OF MALWARE INCLUDE:

- VIRUSES:** malicious software attached to files and programs on infected websites, flash drives (USB), and emails activated by opening the infected application or file.
- WORMS:** malicious software that can transfer and copy itself from computer to computer.
- TRIOLES:** malicious software that looks like a legitimate application or file, installing a user to load and execute the malicious software onto their computer.
- KEYLOGGERS:** malicious software that enables an unauthorized user to gain control of a computer system without being noticed.
- KEYLOGGERS:** malicious software that records keystrokes made by a user in order to gain access to passwords and other personal/financial information.
- RANSOMWARE:** malicious software that blocks access to your organization's system or data until a sum of money is paid.
- SPYWARE:** malicious software that gathers data from your business's devices/systems to take control of its features.
- ADWARE:** software that displays advertisements and redirects your online search requests to advertising websites that collect marketing data about you.

Types of malware can include: covert systems, root or undetected scans, insider charge, and camera activation. Note that some malware can affect your computer or device with no immediate or noticeable symptoms.

What should you do if your business experiences a malware attack?

- Immediately remove infected computers or devices from your business network.
- Consider temporarily taking your network offline to stop the spread of malware.
- Isolate your backups immediately.
- Disable all shared drives that hold critical business information.
- Change all online account passwords and network passwords after removing the system from your network.
- Contact an IT security professional to help mitigate the issue.

Visit [FightCybercrime.org](https://fightcybercrime.org) for more recovery resources.

FightCybercrime.org



CybercrimeSupport.org | FightCybercrime.org | ScanTeam.org
© 2021 Cybercrime Support Network

Thank you.

Cindy Liebes

Chief Program Officer

cindyl@cybercrimesupport.org

CybercrimeSupport.org | FightCybercrime.org | ScamSpotter.org

Find us on:    