


# LIVE SECURITY AWARENESS TRAINING


All Covered   
A PUBLIC SERVICE



-  CYBER CRIME BY-NUMBERS
-  HOW TO SPOT SOCIAL ENGINEERING
-  TOP TACTICS
-  BEST PRACTICES

TAKE-HOME RESOURCES 

LIVE ONSITE/ONLINE 

CAN QUALIFY FOR CE CREDIT 

## WHAT ATTENDEES SAY

**"SERVED IN MILITARY FOR 17 YEARS AND NEVER SAW BETTER TRAINING"**

-BRANDON J., CISO  
NATIONAL INSURER, U.S.

**"OUR STAFF GETS IT, NOW."**

-MICHAEL G, CFO MORTGAGE  
BANKING , U.S.

**"IT WAS LIKE A GOOD NETFLIX BINGE. COULD'VE STAYED ALL DAY."**

-AMANDA C, SVP  
CREDIT UNION, U.S.

**"OUTSTANDING. IT MADE US CARE ABOUT SECURITY"**

-BRENDA K., COO  
MANUFACTURER, CHICAGO AREA

**"WE WERE ENGAGED THE WHOLE TIME. SHOCKING AND FUN. HAVING YOU BACK AGAIN!"**

-ALLYSON B, VP  
PHARMA MANUFACTURER

**"IT SOCIALIZED CYBERSECURITY IN PLAIN TERMS. WE UNDERSTAND AND IT MADE AN IMPACT ON US."**

-TOM W, PARTNER  
MIDWEST CONSULTING FIRM

**SET UP YOUR  
CUSTOM  
TRAINING TODAY!**

CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



**FIND OUT MORE**



# All Covered TAKE HOME RESOURCES



Podcast &  
Newsletter



## PERSONAL PRIVACY CHECKLIST

- Freeze Credit (Yours and Children)
- Strengthen & Manage Passwords (length is key.)
- NEVER RE-USE Passwords)
- Check which Passwords have been compromised and Change them now.
- Restrict sharing details on social media/online (don't submit quiz responses on social, or photos showing GEO etc.)
- VPN and Battery Charger while traveling (avoid plug-stations)
- Practice Phish Spotting (hover mouse)
- Don't open attachments unless verified.
- Enable MFA on everything
- Review Privacy Settings
- Reject Cookies

- Timely Update firmware/software
- Don't Use Free WIFI
- Protect physical risk and report lost devices
- Request Removal of your data from Data Brokers
- Always verify all images, sound and video you see independently before trusting them or spreading misinformation (deepfake dangers)
- Review and Adjust Privacy settings on Apps
- Turn off WIFI and Bluetooth (Airdrop on iOS) unless actively using.
- Don't save passwords in browsers (Chrome if you must) Pause all urgent requests/verify all transmits of private data

CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



FIND OUT MORE



# All Covered TAKE HOME RESOURCES

Podcast &  
Newsletter



## PROTECT YOURSELF AND YOUR FAMILY FROM FINANCIAL HARM



### Freeze Your Credit & Children's Credit

Credit Freeze Guide <https://inteltechniques.com/freeze.html>.

Equifax (<https://www.equifax.com/personal/credit-report-services/> 1-800-349-9960)

TransUnion (1-888-909-8872 <https://www.transunion.com/credit-help>) and

Experian (1-888-397-3742 <https://www.experian.com/help/>)

### Credit Freeze Guide



### Data Removal Guide

### Credential Exposure Removal Guide

### Archive Site Removal Guide



### Been Part of Breach? <https://HavelBeenPwned.com>

### How to protect yourself when booking Travel online

<https://www.getsafeonline.org/personal/articles/holiday-and-travel-booking/>



### Test Your Password <https://security.org/how-secure-is-my-password/>

Remove PII Data Broker. <https://isapps.axiom.com/optout/optout.aspx>



### Verify Before You Buy <https://www.scamadviser.com/>



### Check websites to see if SCAM. <https://www.getsafeonline.org/checkawebsite/>

### Shop Privately/Virtual Cards. <https://privacy.com>



### Health Records Accuracy. <https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html>



### Was a Company Been Breached? <https://breachdirectory.org/>

Is this a Phish? Check if link is phishing: <https://check.getsafeonline.org/>

CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



**FIND OUT MORE**





# All Covered TAKE HOME RESOURCES

Podcast &  
Newsletter



## Protecting Children Online



Concerned about Children and Sextortion?

Remove explicit online photos

How to report Sextortion



## How to protect during ONLINE GAMING

<https://www.getsafeonline.org/personal/articles/online-gaming/>

## How to protect yourself when booking Travel online

<https://www.getsafeonline.org/personal/articles/holiday-and-travel-booking/>



## Protection Guide for Online Dating

<https://www.getsafeonline.org/personal/articles/online-dating/>



## Need to Notify the FBI or FTC?

FBI IC3 <https://www.ic3.gov/Home/ComplaintChoice/default.aspx/>

FTC [ftc.gov/](https://www.ftc.gov/)



## Is this a Phish?

Check if link is phishing: <https://check.getsafeonline.org/>

Use this tool to monitor and discover devices connected to your network

<https://community.fing.com/>

## CIS Hardware and Software Asset Tracker

Use this spreadsheet to track your hardware, software, and sensitive information.

<https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet>

CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



FIND OUT MORE





# All Covered TAKE HOME RESOURCES

Podcast &  
Newsletter



## Google Privacy Protection



1. How to remove your sensitive contact details from Google and reduce call and text spam\*

2. Google your name plus the words "phone number", "email address", or "address".

3. Do you see your sensitive personal info on data brokerage sites?



4. Google has a tool to request a takedown of that info from Google itself (but doesn't remove it from the other sites).

5. Steps for Google removal request:

6. - click the three vertical dots next to the Google results you want removed



7. - click "remove result"

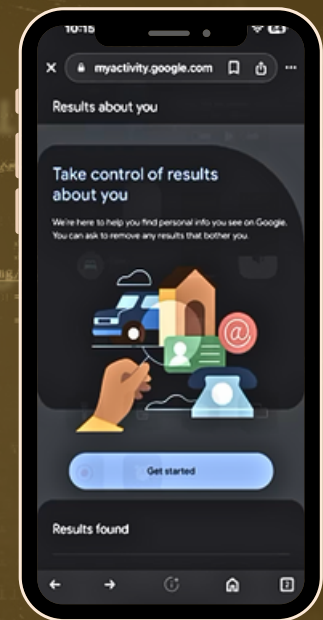
8. - click "it shows my personal contact info", following remaining steps

9. Sometimes Google approves the removal, sometimes they don't.



10. The info still exists outside of Google.

11. There are tools available to remove details on the data brokerage site itself over time including DeleteMe! 20 employees, 2+ servers. PEN TESTING-ALL (but what type?)



CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



FIND OUT MORE





# All Covered TAKE HOME RESOURCES

Podcast &  
Newsletter



## Cyber Insurer Checklist

-  **Managed Endpoint Protection**
-  **Managed Security Information & Event Monitoring**
-  **Incident Response Plan/Playbook/Tabletops**

### EMAIL SECURITY

- Domains with Email Enabled**  
Identify and document the email domain along with verification of DNS Mail Exchange (MX) details, SPF, DKIM and DMARC configurations
- Advanced Threat Protection**  
Identify and confirm the email filtering service, and that it is enabled and properly configured to scan attachments, validate links and prevent phishing.

### DOMAIN & WEBSITE SECURITY

- Website Domains**  
Identify the primary corporate domain(s), subdomains and document DNS and expiration dates

### BACKUPS

- Workstations & Servers with Backups Present**  
Identify the cloud provider and verify if recent backups have occurred, are encrypted, and have completed in the last 30 days
- Test Backups**  
Verify if a successful restoration of backup data has been performed in the last 6 months

### NETWORK

- Segmentation**  
Verify if the network is segregated between public and trusted networks via properly configured Access Rules and NAT policies

### Coverage Risks & Defenses

**Failure to Maintain** This clause enables insurance providers to limit coverage if evidence suggests the policyholder's organization is improperly maintained, and kept secure with the basic security controls identified in this document.

**Neglected Software Vulnerabilities** Threat actors will often seek to exploit software that is out-of-date or unpatched. Insurance carriers expect the policyholder to practice proper cyber hygiene and maintain the latest secure versions. They may provide a grace period, but once lapsed, will require co-insurance and progressively reduce the coverage amount if the software is exploited in an incident.

**Safe Harbor Laws** In the wake of a breach, if an organization can prove that they have a cyber program, and reasonably conform to established standard frameworks such as NIST, ISO 27001, or CIS, these laws can provide an affirmative defense to liability caused by the breach.

### AUTHENTICATION & MFA

- Multi-factor Authentication (MFA)**  
All user email accounts should have MFA enforced
- Privileged Users**  
Verify privileged accounts are separated

### WORKSTATIONS & SERVERS

- Encryption at Rest**  
Verify that drives are encrypted with Bitlocker on Windows or FileVault on Macs
- Remote Desktop Protocol Disabled**  
Verify if RDP is allowed on workstations and servers
- Endpoint Protection, Anti-Virus, Anti-Malware**  
Identify the endpoint protection and AV provider, and whether it is properly installed, activated, and up-to-date
- Domain, Public, Private Firewalls**  
Verify all devices have local firewalls enabled
- Supported Software**  
Verify if any software being used has reached end-of-life

CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



**FIND OUT MORE**



# All Covered TAKE HOME RESOURCES

Podcast &  
Newsletter



## OPERATION PRIVACY

STEP BY STEP GUIDES TO PROTECT YOUR INDIVIDUAL PRIVACY AND REMOVE DATA

<https://www.operationprivacy.com/>



- Data Brokers Opt-Out List
- Data Retrieval
- Credit Freezes
- OpSec Tips
- Device Privacy
- Private Forum Access
- VoIP Suite

A screenshot of the Operation Privacy dashboard. The title is 'Operation Privacy' with the subtitle 'A DIY dashboard: Because it's personal'. Below that is a yellow banner that says 'Prevent stalking, doxing, swatting, and take control of your online identity'. There is a 'Get Started' button with a magnifying glass icon. To the right is a laptop displaying a dashboard with various charts and graphs. Below the screenshot is a box titled 'Privacy Dashboard' with a list of features: Self-Managed, 400+ tasks, Privacy Score, Crowd Sourced, Track Progress, Continuous Updates, Private And Secure, Proactive Monitoring, and Used By Pros.

**Operation Privacy**  
A DIY dashboard: Because it's personal

Prevent stalking, doxing, swatting, and take control of your online identity

Get Started

**Privacy Dashboard**

- Self-Managed
- 400+ tasks
- Privacy Score
- Crowd Sourced
- Track Progress
- Continuous Updates
- Private And Secure
- Proactive Monitoring
- Used By Pros



**Need Info on People or an Organization?**  
Ultimate OSINT Resources. Conduct your Own OSINT



(Open-Source Intelligence Investigation)  
<https://start.me/p/DPYPMz/the-ultimate-osint-collection>



CONTACT:  
DAVID MAURO  
DMAURO@ALLCOVERED.COM



**FIND OUT MORE**

