All Covered Cybersecurity Insight

KONICA MINOLTA

MIT NA | MANAGED IT NORTH AMERICA

Take-Home RESOURCES

You/Family

Organization

BEST PRACTICES

See Something
Say Something

- Freeze Credit
- MFA on Everything
- Strong PW Management
- Reject Cookies
- Remove Data Broker Access
- Learn To Spot Phish
- No Public WIFI
- No Public Charging
- *See Something Say Something*

Individual

Organization

1. Network 24/7 Eyes-on-Glass

   Real-time Detection/Response
2. Endpoint Detection/Response
3. Vulnerability Mgmt.
4. Social Engineering Training
5. WISP/IR Plan/Tabletops

Policies:

Vendor Management, AI, Compliance
WISP

Top Ways To 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 (1-888-909-8872https://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://HaveIBeenPwned.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.acxiom.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/

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/

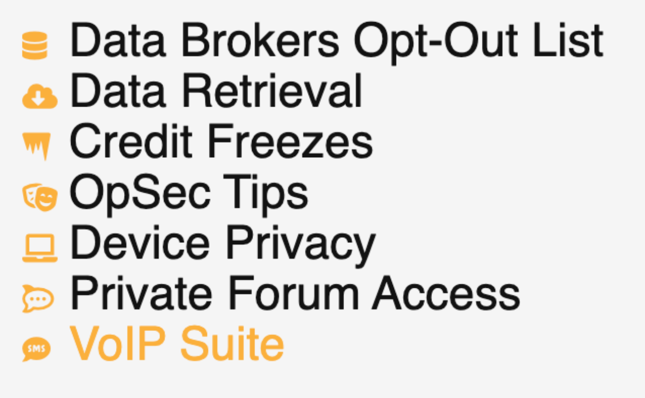
For More Contact David Mauro
Dmauro@allcovered.com

KONICA MINOLTA | MIT NA MANAGED IT NORTH AMERICA

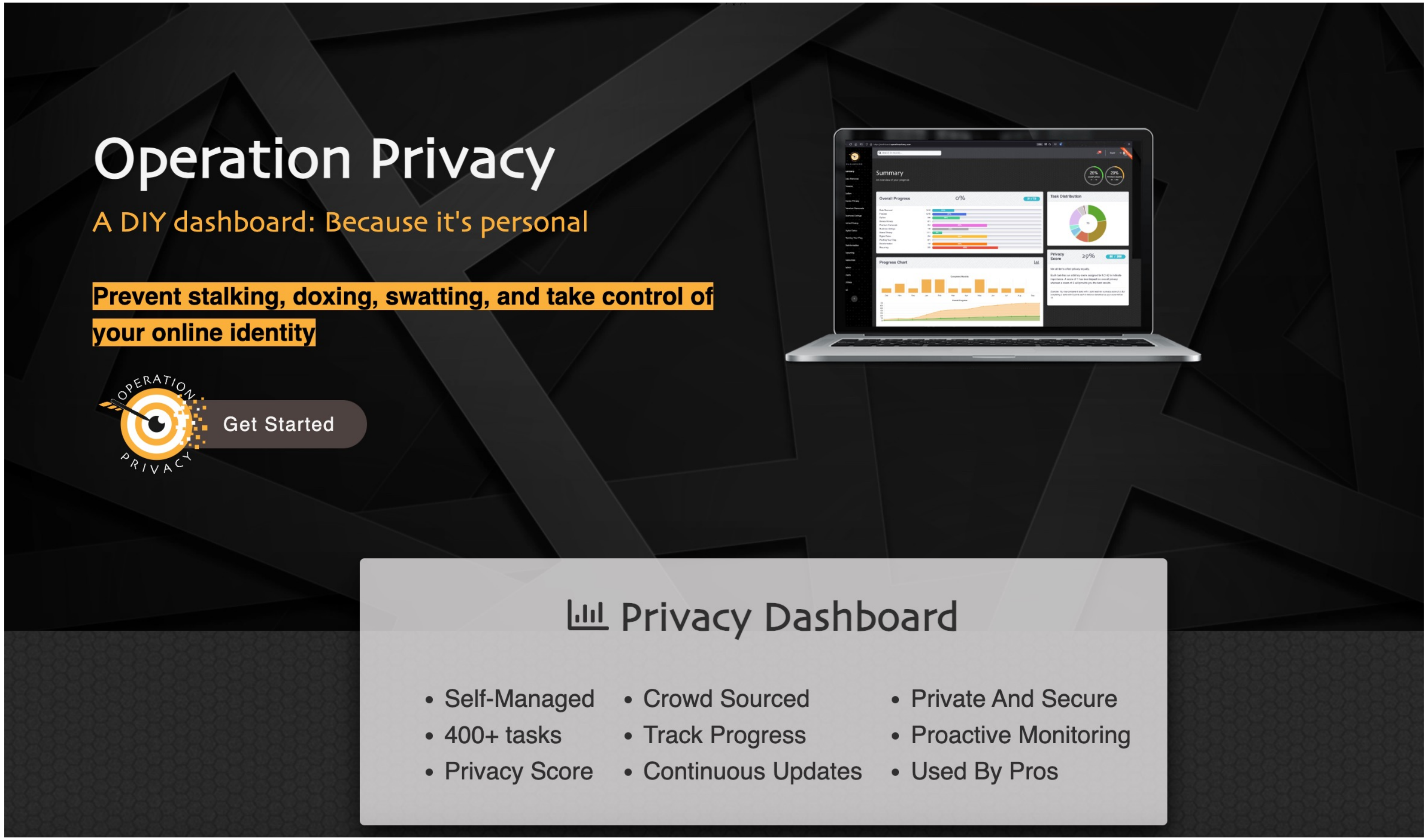
Operation Privacy

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



Operation Privacy

A DIY dashboard: Because it's personal

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

Privacy Dashboard

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

Useful Guides for Company

CISA/FBI RANSOMWARE GUIDE

https://www.cisa.gov/stopransomware/ransomware-guide

CISA/FBI New PHISHING GUIDE

https://www.cisa.gov/news-events/news/cisa-nsa-fbi-ms-isac-publish-guide-preventing-phishing-intrusions

Data Request Guide

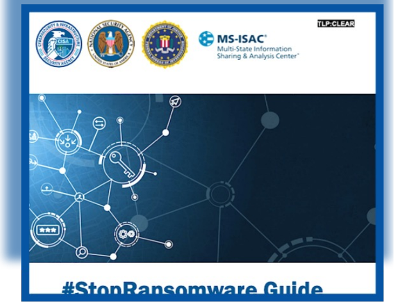
Firewall Guide
VPN Guide

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



TLP:CLEAR

MS-ISAC
Multi-State Information
Sharing & Analysis Center

#StopRansomware Guide

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

For More Contact David Mauro
Dmauro@allcovered.com

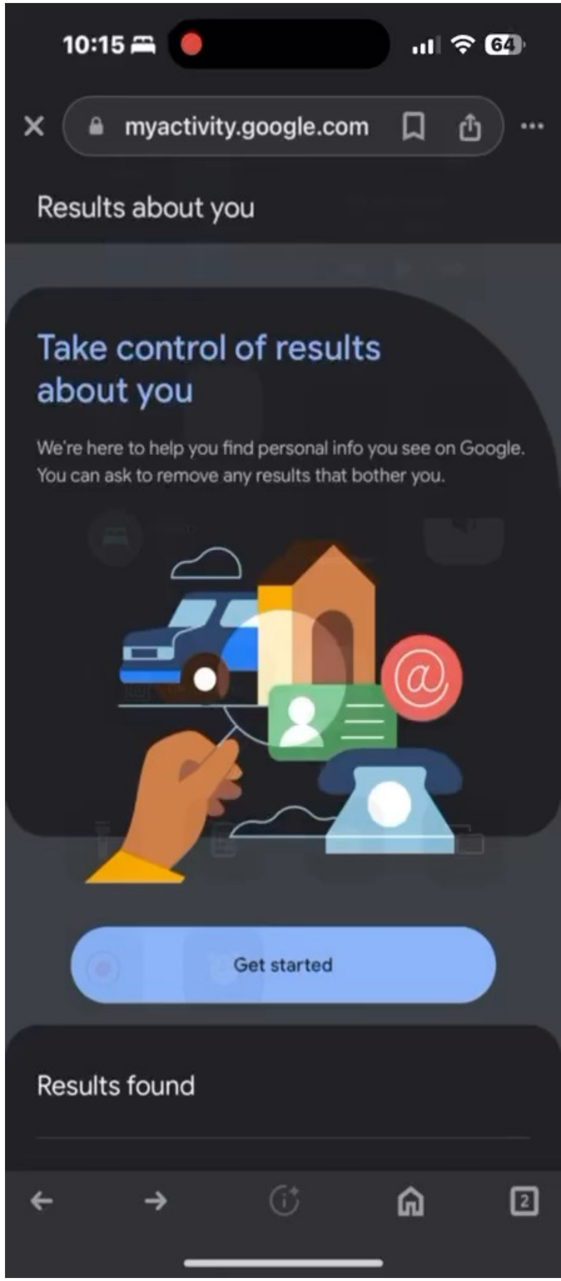
KONICA MINOLTA | MIT NA MANAGED IT NORTH AMERICA

Google Privacy Protection

KONICA MINOLTA
MIT NA | MANAGED IT NORTH AMERICA

Hot to Remove Your Sensitive Contact Details From Google

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?)



Results about you

Take control of results about you

We're here to help you find personal info you see on Google. You can ask to remove any results that bother you.

Results found

Social Engineering

Red Flags

FROM

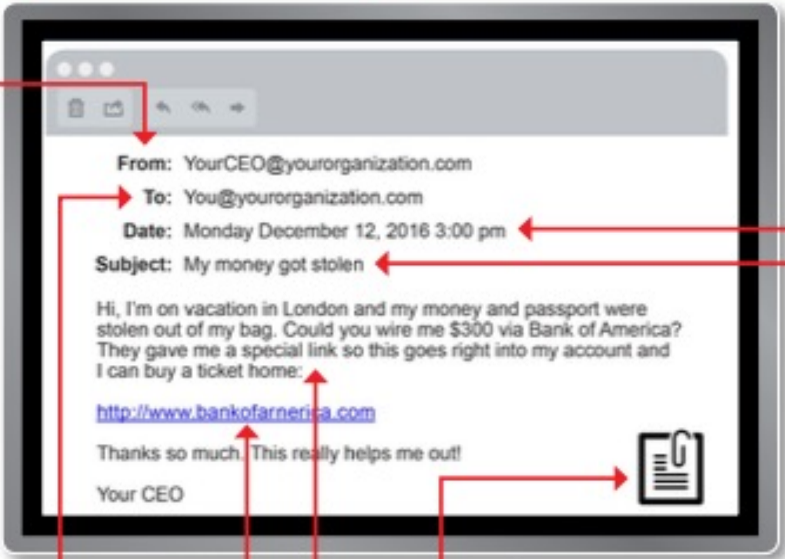
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



From: YourCEO@yourorganization.com

To: You@yourorganization.com

Date: Monday December 12, 2016 3:00 pm

Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Security Awareness Tool Kits-(No Cost)

- Cybersecurity Infrastructure Security Agency (CISA) https://www.cisa.gov/cybersecurity-awareness-mont
- INFOSEC Toolkit https://www.infosecinstitute.com/iq/cybersecurity-awareness-month/
- SANS Institute Toolkit. https://go.sans.org/lp-cybersecurity-awareness-month-kit
- KnowB4 Toolkit: https://www.knowbe4.com/cybersecurity-resource-kit-ga
- National Children Alliance Toolkit https://learn.nationalchildrensalliance.org/csec-resource-toolkit-sexual-images-resources

Company Cyber Insurance Checklist

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 segregrated between public and trusted networks via properly configured Access Rules and NAT policies

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

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 policy-holder 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 an 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.

For More Contact David Mauro
Dmauro@allcovered.com

KONICA MINOLTA | MIT NA MANAGED IT NORTH AMERICA

KONICA MINOLTA
MIT NA | MANAGED IT NORTH AMERICA

THANK YOU!

For More Contact David Mauro
Dmauro@allcovered.com