ALL COVERED
A KONICA MINOLTA DIVISION

Podcast &
Newsletter

Stay Current
Top Tactics
Best Practices

TAKE HOME RESOURCES

CONTACT:
DAVID MAURO
DMAURO@ALLCOVERED.COM

WWW.CYBERCRIMEJUNKIES.COM

FIND OUT MORE

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

TAKE HOME RESOURCES

ALL COVERED
A KONICA MINOLTA DIVISION

Podcast & Newsletter

REDUCE YOUR FOOTPRINT

RISKS

- Most people have old email accounts on social platforms (remember MySPace, Friendster, Tumblr, AOL or YAHOO etc)
- Many People have confidential/sensitive docs in their emails (sent folder, archived folders).
- Most people have security questions that are for sale on dark web through prior breaches)
- Most Companies do not off board former employees fast enough, leaving access open
- Most People Re-Use a really good password. A Major cuase of data breaches.
- Most organizations do not hold LIVE Lunch and Learns on Cyber Awareness Often ENough and threats change so old session becaome outdated.

STEPS TO TAKE

- Inventory old accounts. Reset old PW's then Delete unused accounts.

  Do EMAIL SWEEP and remove/save all older sensitive docs/files etc outside email system.
- Create New Inveted (fictional) security questions only you know. Like being a Spy :) Otherwise too easy to find them.
- Leaders must offboard employees fast, removing access to all systems and deleting accounts.
- Never Re-Use ANY Password-even great ones. Use a Password Manager or simple Algorithm we can show you.
- Hold Monthly/QUarterly Security Lunch/Learns/Webinars etc. We offer those at NO COST.

CONTACT:
DAVID MAURO
DMAURO@ALLCOVERED.COM

FIND OUT MORE

TAKE HOME RESOURCES

Podcast & Newsletter

PROTECT YOURSELF AND YOUR FAMILY FROM FINANCIAL HARM

- [x] 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/)
- [x] Credit Freeze Guide
  Data Removal Guide
  Credential Exposure Removal Guide
  Archive Site Removal Guide
- [x] 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/
- [x] Test Your Password https://security.org/how-secure-is-my-password/
  Remove PII Data Broker. https://isapps.acxiom.com/optout/optout.aspx
- [x] Verify Before You Buy https://www.scamadviser.com/
- [x] Check websites to see if SCAM. https://www.getsafeonline.org/checkawebsite/
- [ ] Shop Privately/Virtual Cards. https://privacy.com
- [x] Health Records Accuracy. https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html
- [x] 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

TAKE HOME RESOURCES

ALL COVERED
A KONICA MINOLTA DIVISION

PODCAST & NEWSLETTER

Children Online?

Concerned about Children and Sextortion?
Remove explicit online photos
How to report Sextortion

ONLINE GAMING?

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

TRAVELING?

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

Good Tip: When leaving an OOO Auto-reply email only say "I am currently out of office. Please expect a delay in response."
*****Do Not disclose timeline, co-workers or other details.**

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/

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/

Track/Inventory Your Devices & Software

Sample 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

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

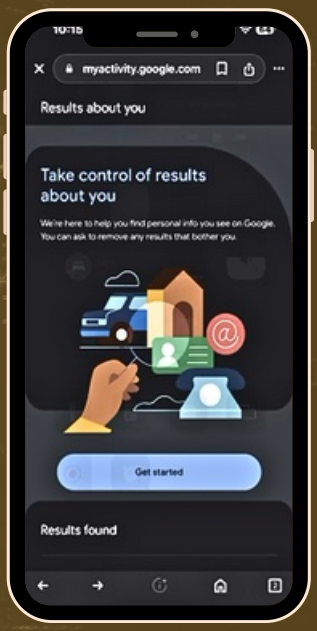
7.- click "remove result"

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

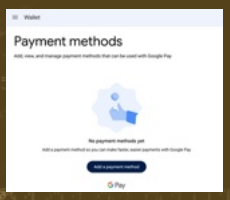
FIND OUT MORE

TAKE HOME RESOURCES

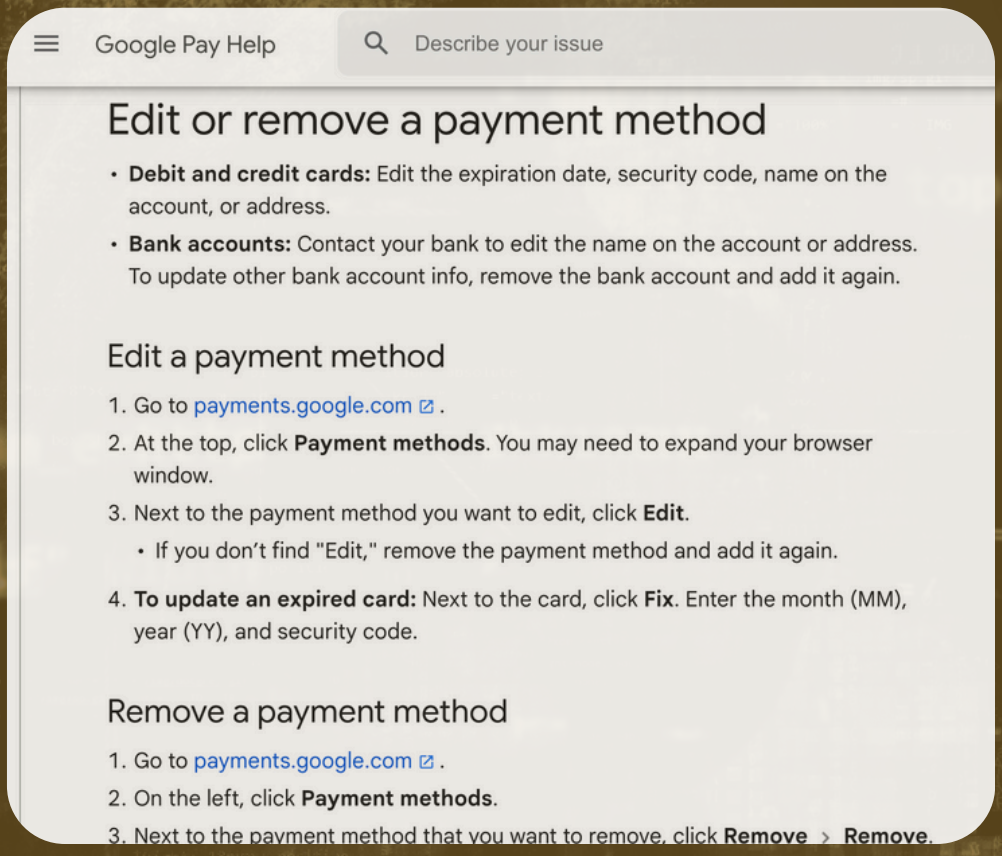
Podcast & Newsletter

Remove Your Credit Cards/Payment from Web Browsers (Like Google CHROME)

- [x] **Go into your Google Account>Wallet and REMOVE ALL CARDS until your see this:**



- [x] **Go To Google Play and remove CARDS**



Google Pay Help

Describe your issue

Edit or remove a payment method

- **Debit and credit cards:** Edit the expiration date, security code, name on the account, or address.
- **Bank accounts:** Contact your bank to edit the name on the account or address. To update other bank account info, remove the bank account and add it again.

Edit a payment method

1. Go to payments.google.com .
2. At the top, click **Payment methods**. You may need to expand your browser window.
3. Next to the payment method you want to edit, click **Edit**.
   - If you don't find "Edit," remove the payment method and add it again.
4. **To update an expired card:** Next to the card, click **Fix**. Enter the month (MM), year (YY), and security code.

Remove a payment method

1. Go to payments.google.com .
2. On the left, click **Payment methods**.
3. Next to the payment method that you want to remove, click **Remove** > **Remove**.

CONTACT:
DAVID MAURO
DMAURO@ALLCOVERED.COM

- [x]

FIND OUT MORE

TAKE HOME RESOURCES

ALL COVERED
A KONICA MINOLTA DIVISION

Podcast &
Newsletter

OPERATION PRIVACY

STEP BY STEP GUIDES
NDIVIDUAL PRIVACY AND REMOVE DATA

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

https://www.operationprivacy.com/

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

TAKE HOME RESOURCES

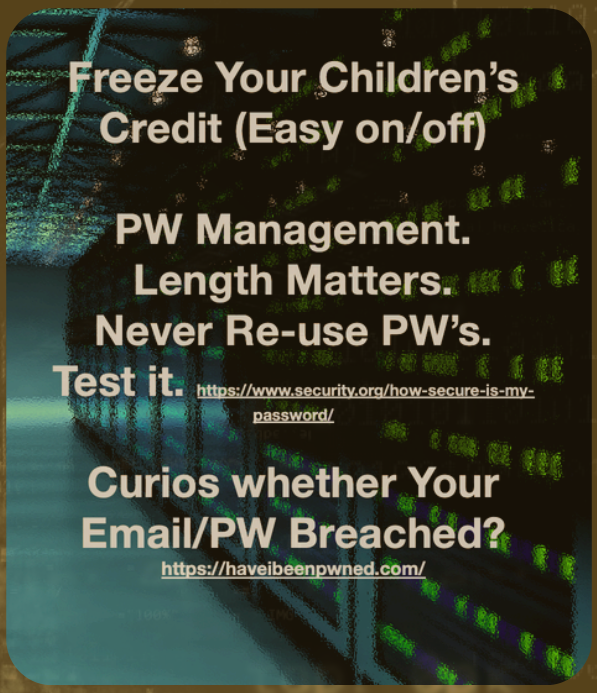
ALL COVERED
A KONICA MINOLTA DIVISION

Podcast & Newsletter

INDIVIDUALS

Freeze Credit
Manage Passwords
Reject Cookies
Adjust Privacy Settings
Verify Independently
Pause/Amygdala Hijack

See Something?



Social Media & More

Adjust Privacy/GEO OFF
Only Post Photos w/o Info
Enable MFA
No "Auto connect to WIFI"
Learn How To Report/Block
Reset Phone Weekly/Update OS
Post After Vacation
Don't Answer Quizzes
Don't Reshare until Verified
Beware of Ads.
Beware Apps

Traveling? Use Battery Pack.
Beware of Juice Jacking
Never use Free Public WIFI.

ORGANIZATIONS

Real-Time Detection
Endpoint Det/Resp-EDR
IR Playbook/Tabletops
Ongoing Education/Testing
Vendor Management/3rd Partie
VMP/Pen-Testing/Adversary Emulation

Say Something!

WANT TO STAY CURRENT?
SUBSCRIBE FOR FREE

WWW.CYBERCRIMEJUNKIES.COM

CONTACT:
DAVID MAURO
DMAURO@ALLCOVERED.COM

FIND OUT MORE

TAKE HOME RESOURCES

ALL COVERED
A KONICA MINOLTA DIVISION

Podcast & Newsletter

Organizational Cyber Checklist

- [x] **Managed Endpoint Protection**
- [x] **Managed Security Information & Eevent Monitoring**
- [x] **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 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.

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