

Helping Elderly Activists Improve their Security



Kris Hardy
@nonlinear@mastodon.nz
hardyrk@gmail.com

Thank You to Our Sponsors and Hosts!



BASTION

SECURITY GROUP



DATACOM



84.



PentesterLab

plexure

VERACODE

Without them, this Conference couldn't happen.

Disclaimer

This talk is not endorsed by AppSec NZ, any sponsors, or my past, present or future employers.

I am not an attorney. Please seek advice from a lawyer if you have legal questions.

Scenario

A friend lost \$100k to a tech support scam.

They are in their 80's and retired.

What do you do?

What would you have told them to do to prevent this?

Would they have followed your advice?

Scenario #2

Another friend is in their 80's and is a long-time peace activist.

They are still involved in direct action and occasionally get arrested for civil disobedience.

They ask you for advice on how to protect their communications.

What do you tell them?

Will they follow your advice?

Scenario #3

What of both of these people are actually the same person?

What do you do and what would you recommend?

Inspiration



Lesley Carhart

May 18

@hacks4pancakes@inf...

As the Person Who Gets asked a lot, Meta's "go it alone yourself" response to account hacking / theft is still utterly crazy.

Lesley Carhart, Director of IR at Dragos
@hacks4pancakes@infosec.exchange



evacide

Apr 1

@evacide@hacyderm.io

I have experimented with privacy/security advice chatbots and I have discovered that the part of my expertise I absolutely cannot replicate is figuring out what the person I'm talking to isn't telling me.

Eva Galperin, Director of Cybersecurity at EFF
@evacide@hacyderm.io

norton

- Download & install
- Buy & Renew
- Threat Removal
- Protect Windows and Mac devices
- Norton Secure VPN
- Protect Android and iOS Devices

Other products

Verify that an email you receive from Norton is legitimate

We use email or direct mail to keep you informed about the latest offers, announcements, and product updates from Norton. Norton Affiliates may also send emails or mails about various offers or promotions on Norton products. These may contain trademarked Norton images, but your personal information is not used to send these mails. You should never provide personal or confidential information to a sender or webpage that you do not know or trust.

⚠️ Sometimes you may receive mails from cybercriminals claiming that it is from Norton. If you receive suspicious mails that look like it is from us, forward it as an attachment to spam@norton.com. To know more, read [Cyber scans and how to avoid them](#).

Here is a list of legitimate Norton domains for your reference. You can use your browser search (press Ctrl + F key or Command + F key) and type the domain to see if it is listed here.

For example, if you received an email from noreply@norton.com, open your browser search and type norton.com. If the domain is listed here, the email you received is a legitimate Norton email.

- @norton@klook.com
- @norton.com
- @identity.norton.com
- @login.norton.com
- @securenorton.com
- @secure.norton.com
- @klook.norton.com
- @mylogin.norton.com
- @myidentity.com
- @family.norton.com
- @klook.com
- @mail.nortonstore.ir
- @mail.nortonstore.jp
- @mail.nortonstore.kh
- @mail.nortonstore.kr
- @mail.nortonstore.mx
- @mail.nortonstore.sg
- @mail.nortonstore.us
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @email.norton.com
- @identityprotection.norton.com
- @subscriptions.norton.com
- @ubiservico.com
- @winelogs.com
- @tracelot.com
- @call-norton.com
- @m.onetrust.com
- @cleverbridge.com
- @creditview.co.uk

29 domains!?!?



**UNIFIED
UNITED STATES
DEPORTED
VETERANS
"LEAVE NO ONE BEHIND"**



**DARKNET
DIARIES**

Inspiration



Lesley Carhart

@hacks4pancakes@inf...

May 18

As the Person Who Gets asked a lot, Met
"go it alone yourself" response to
hacking / theft is still uttered

Lesley Carhart
@hacks4pancakes



evacide

@evacide

Lb

Community Infosec is an
UNSOLVED PROBLEM

STATES
SUPPORTED
VETERANS
"LEAVE NO ONE BEHIND"



The current state of advice to individuals

Be suspicious of scam/malicious emails and messages

Use a password manager

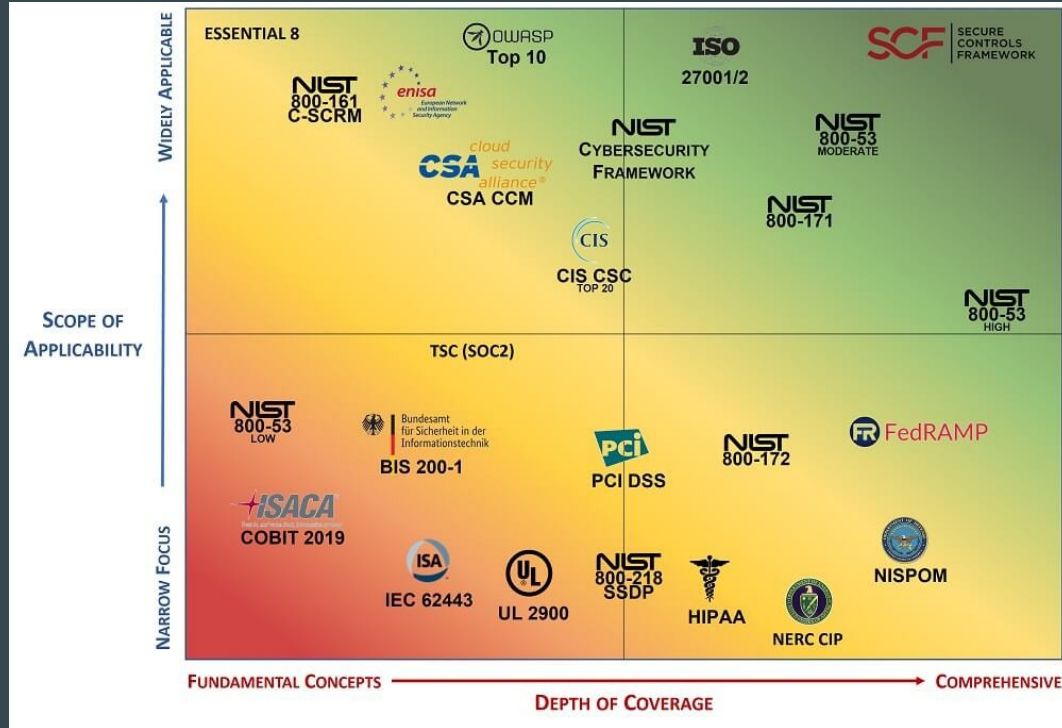
Turn on MFA

Enable device encryption

Use an up-to-date browser w/ some security extensions

Keep software up-to-date

If your friend was an enterprise...



NIST SP-800-53
- 1190 controls

FedRAMP
- 156 controls (Low Baseline)

Secure Controls Framework
- 1234 controls

<https://complianceforge.com/scf/secure-controls-framework-scf-download/>

If your friend was an enterprise...

MFA

DLP / Proxy

Training

Canaries

Behavioural EDR /

SIEM / SOAR

Antivirus / Antimalware

Threat Feeds / Malware

MDM / Patch compliance

Free Networks

VPN / CASB

Security Operations

Centre / MSSP

If your friend was an enterprise...

MFA

DLP

Training

Behavioural EDR

SIEM / SOAR

Antivirus / AV

Threat Feeds / Malware

MDM

Insurance

Free Networks

CA

Security Operations

Centre / MSSP

Who pays for this?

If your friend was an enterprise...

MFA

DLP

Training

Behavioural EDR

SOAR

Antivirus / AV

Malware

MDM

Finance

Free No

CA

Security Operations

Centre / MSSP

Who manages this?

Who pays for this?

If your friend was an enterprise...

MFA

DLP

Training

Who manages this?
Can they be trusted?

MDM

Finance

Free No

malware

CA

Security Operat

Centre / MSSP

Who processes this?

If enterprise...

MFA

DLP

Training

Can the support be trusted?

MDM

Finance

Software

Ca

Cent

Who will provide support?

this?

Who P

to

If enterprise...

MFA

Training

Who

Who will answer

"Can I click on this?"

Can I provide

malware

Center

How do risks change if you are an advisor?

Risks to individuals

They must trust you and new systems.

You are in a privileged position.

Risks to you become additional risks to individuals.

Will your controls **help** or **hinder**?

Risks to advisors

You may be privy to sensitive information.

You may become a watering hole target.

You may be targeted by state actors, organisations, and disrupters, depending on who you are working with.

You may have legal liability or be considered as a co-conspirator.

How can we get better? A Practical Risk-focused Approach:

1. Listen to them. **"How can I help?"**
2. Focus on their **immediate needs** first.
3. They own their risk. You can provide **recommendations**.
4. **Accept it** if they don't follow your advice.
5. **Set clear boundaries** and adjust them as necessary. Your morals are your guide.
6. **Avoid paranoia** within yourself and them.
7. **Do your own risk assessment**. Your risks are not their risks, and vice versa.
8. You can help, and trust takes time. **Be as available as possible**.

6 interaction types / roles you might play

Advisor

“Family counselor”

Translator

Intermediary

Advocate

MSSP

Advisor

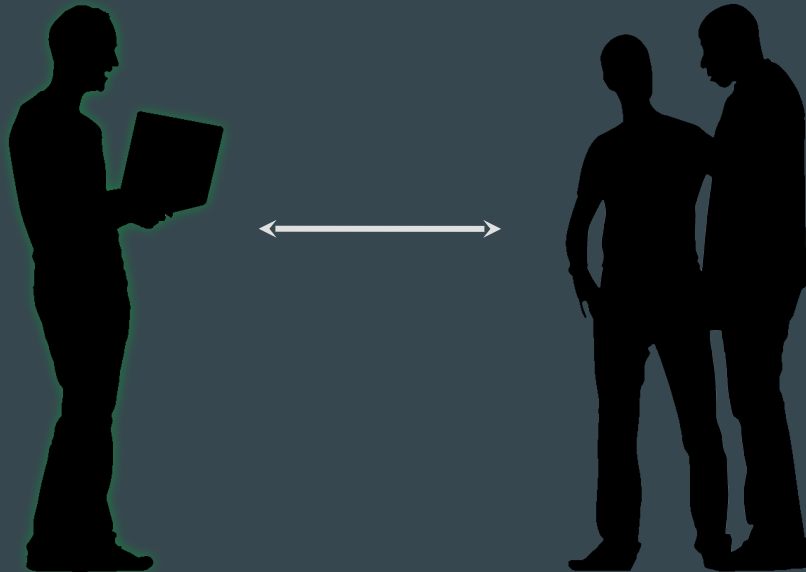
1-1 or 1-group – Work directly with an individual/group.



Family counselor

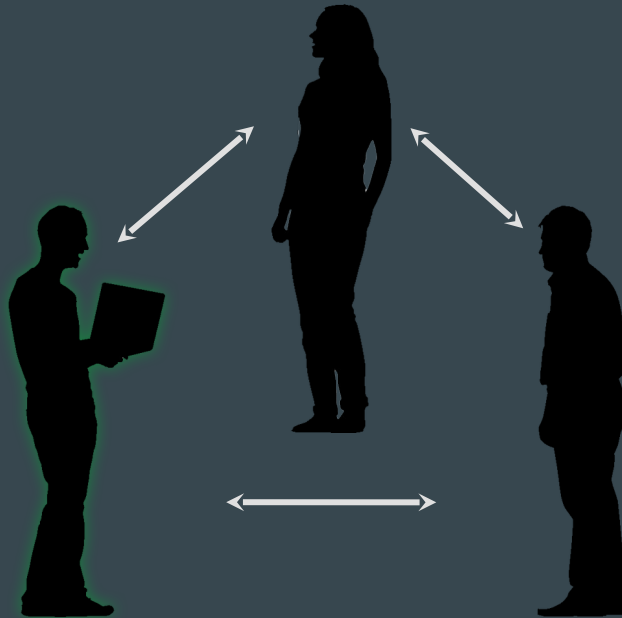
You work with an individual and a concerned person (*ie* family member).

You are there to understand both sides.



Translator

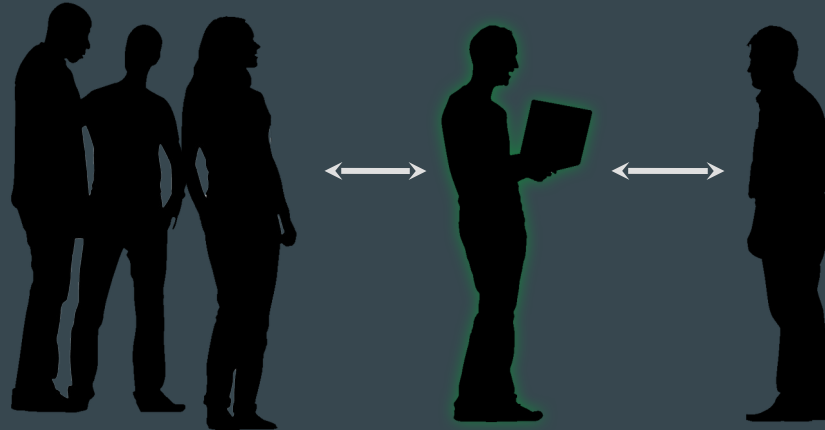
You work with an individual to help them understand what another group/company/family member is saying.



Intermediary

You work with an individual on behalf of a group to help them with their security.

This requires a lot of trust and support time because everything goes through you.

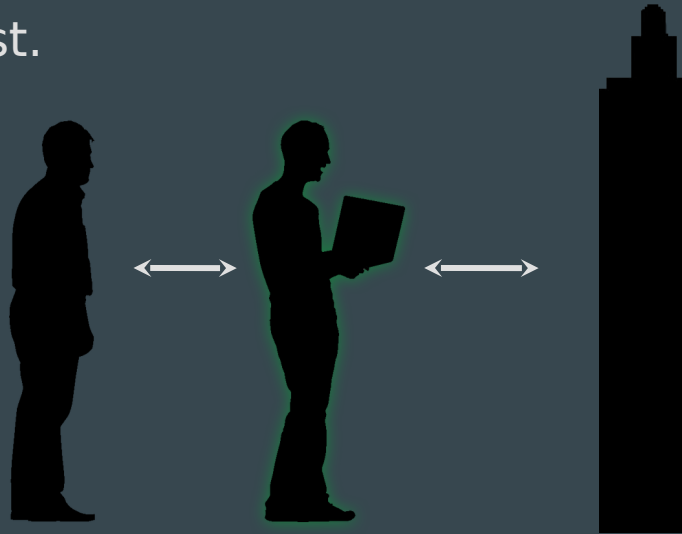


Advocate

Delegated to handle some issues on behalf of the individual.

You have specialized knowledge, right vocabulary, right temperament, etc.

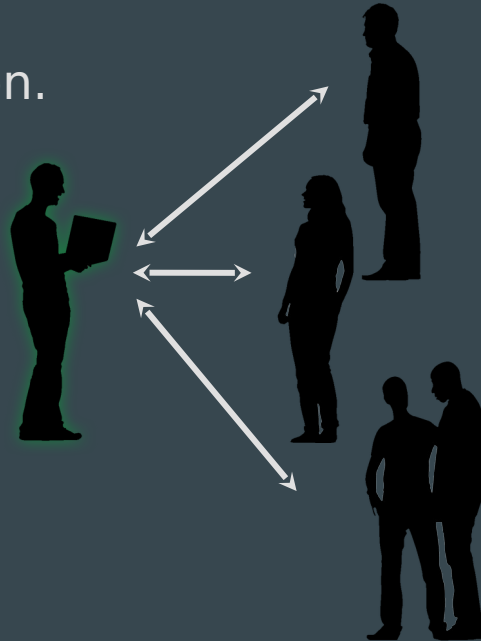
Requires absolute trust.



Managed Security Services Provider (MSSP)

You run security systems and onboard their computer and phone into them.

You are **the** support person.



Valuable Resources

Groups often need “low-tech” more than “high-tech”. An email list was the most valuable thing I set up in my VFP chapter.

Education:

riseup.net – Mailing lists, wikis, VPN

NetSafe - <https://netsafe.org.nz/older-people>

National Council on Aging -

<https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security/>

DigiCert - <https://www.digicert.com/blog/cybersecurity-for-seniors-in-7-steps>

Activist Handbook - <https://activisthandbook.org/tools/security>

Security Gladiators - <https://securitygladiators.com/cybersecurity-for-activists/>

Frontline Defenders - <https://www.frontlinedefenders.org/en/digital-security-resources>

EFF - <https://ssd.eff.org/>

security-in-a-box - <https://securityinabox.org/en/>