Helping Elderly Activists Improve their Security …

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

Thank You to Our Sponsors and Hosts!

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?

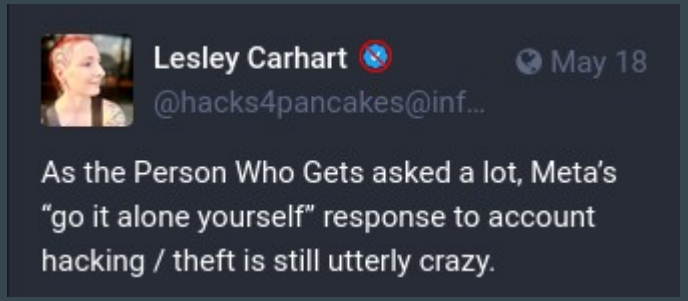
Will they follow your advice?

Scenario #3

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

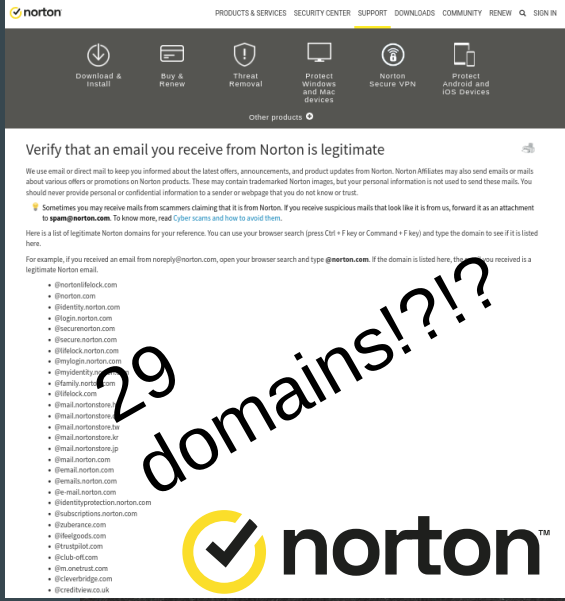
What do you do and what would you recommend?

Inspiration



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

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



Inspiration

Lesley Carha
@hack

y at EFF
n.io

Community Infosec is an UNSOLVED PROBLEM

The current state of advice to individuals

Be suspicious of scam/malicious emails and messages

Use a password manager

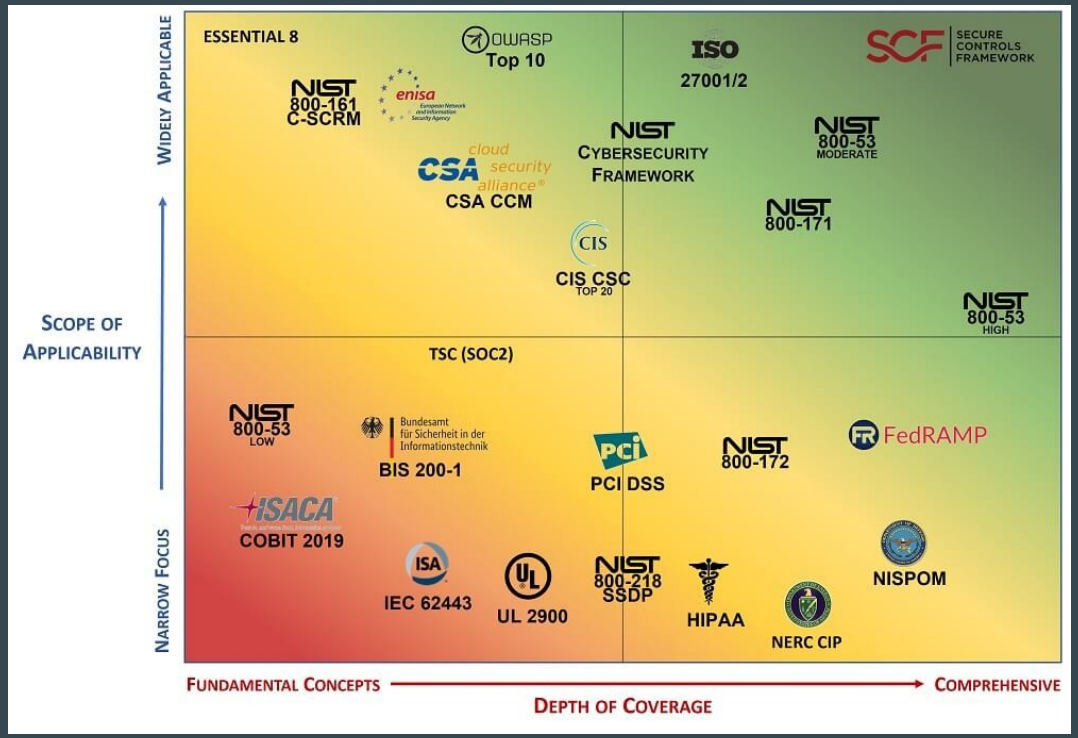
Turn on MFA

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

Training

Behavioural EDR / Antivirus / Antimalware

MDM / Patch compliance

VPN / CASB

DLP / Proxy

Canaries

SIEM / SOAR

Threat Feeds / Malware Free Networks

Security Operations Centre / MSSP

If your friend was an enterprise...

MFA

Training

Behavioural EDR /

Antivirus / A

MDM

CA

DLP

M / SOAR

Threat Feeds / Malware Free Networks

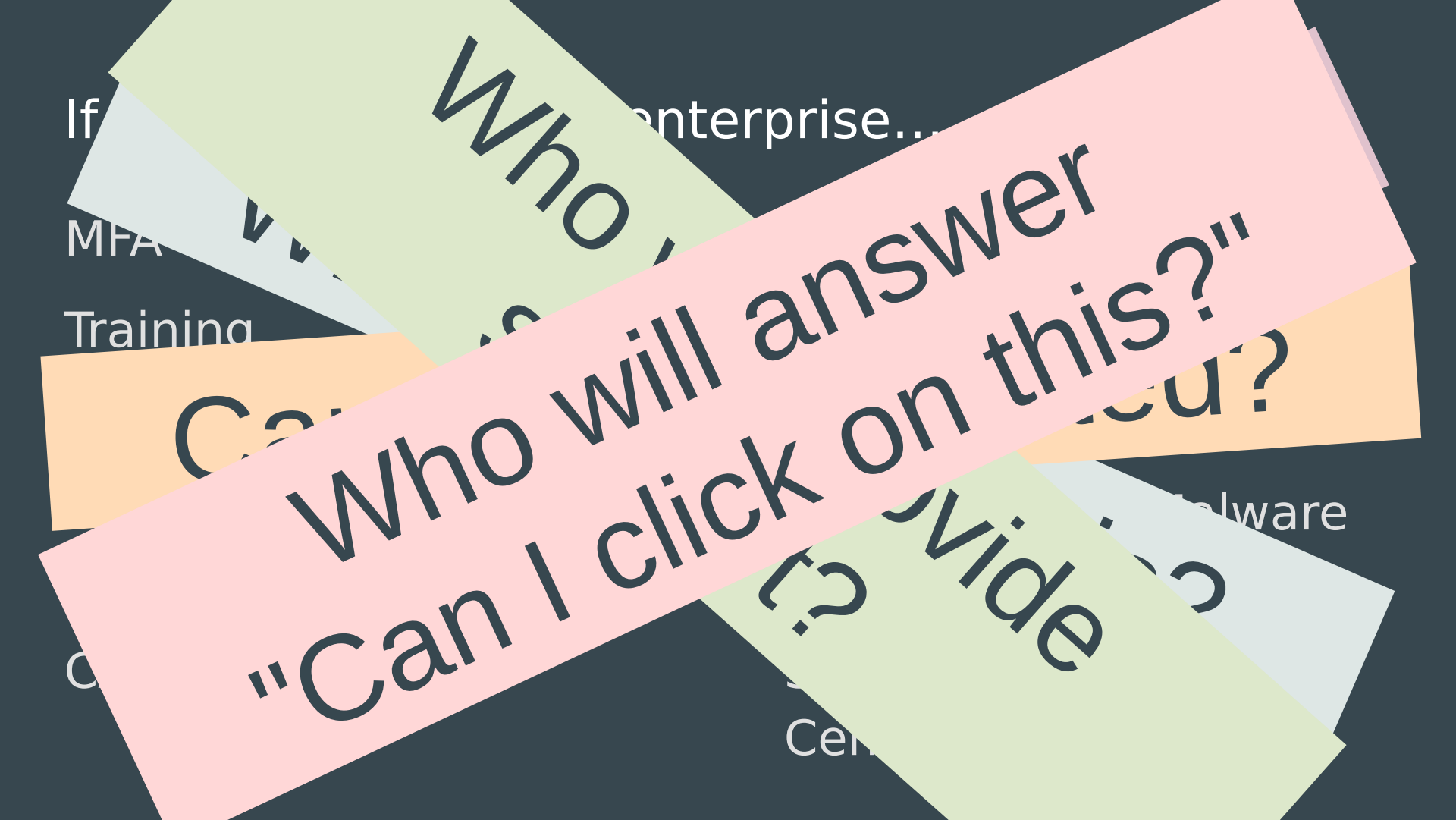
Security Operations Centre / MSSP

Who pays for this?


If iend was an enterprise...
MFA
Training
Behavioural EDR
Antivirus /
MDM
CA
DLP
OAR
lware
Free N
Security Operat
Centre / MSSP
Who manages this?
Who p or this?


If iend was an enterprise...
MFA
DLP
Training
this?
Can they be trusted?
Who p es this?
lware
MDM
Free N
Security Operati
Centre / MSSP


If
enterprise...
MFA
DLP
Training
this?
Can th
usted?
Who p
lware
MDM
iance
CA
Cer
Who will provide support?


If
enterprise...
MFA
Training
Who will answer
"Can I click on this?"
lware
Cer

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

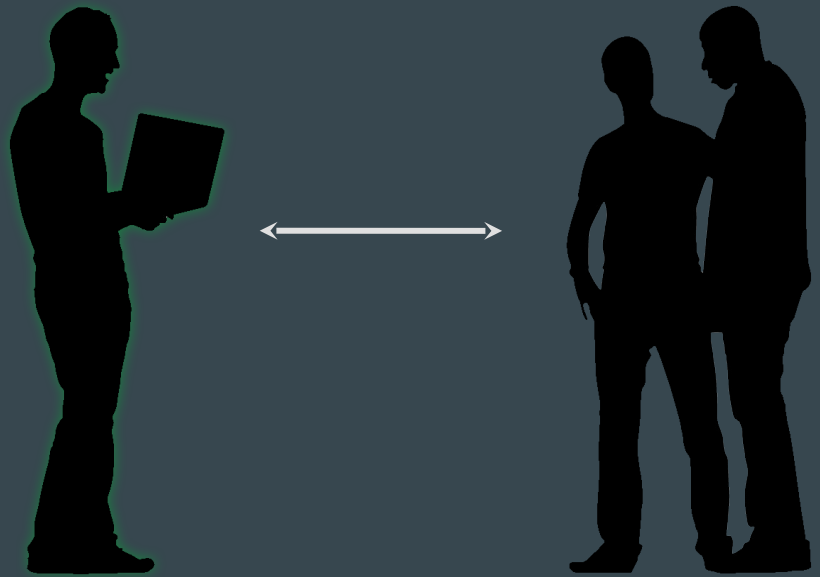
Advisor

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

Family counselor

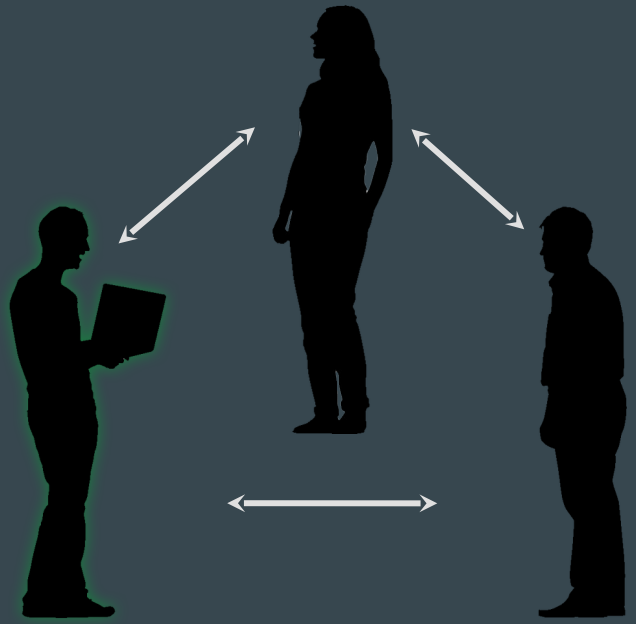
You work with an individual and a concerned person (*ie* family member).

You are there to understand both sides.



Translator

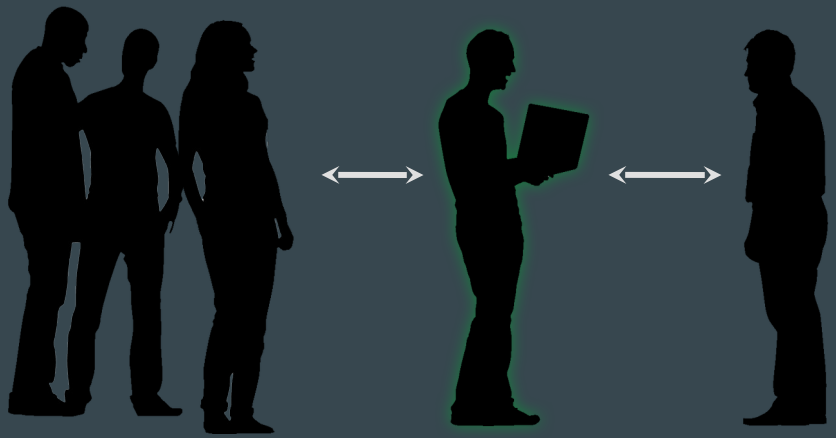
You work with an individual to help them understand what another group/company/family member is saying.



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.

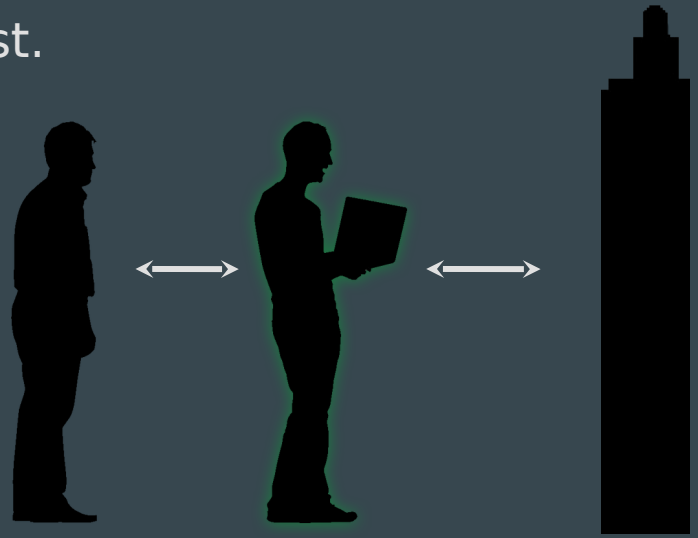


Advocate

Delegated to handle some issues on behalf of the individual.

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

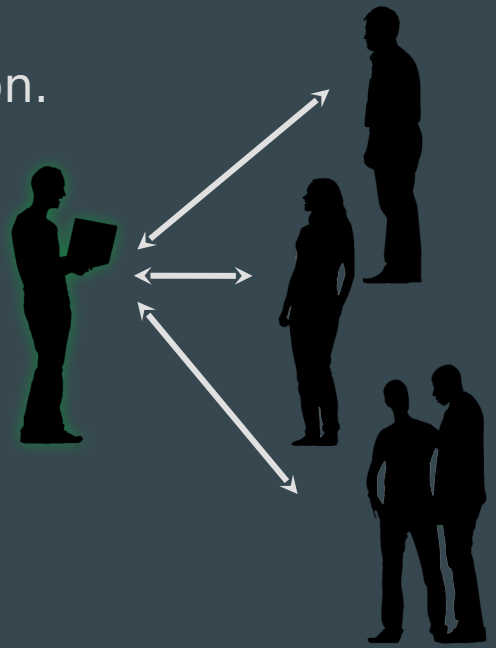
Requires absolute trust.



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/