Human Sensors

https://sans.org/security-awareness
The Problem
The Solution
“Employee notifications were the most common internal discovery method for the second straight year and there was also an uptick in detection through internal financial audits, associated with business email compromise (BEC)."

Verizon DBIR - 2017
What? People are the weakest link, they are the problem – not the solution.
Technology vs. Human Investment

Resources

Laptop

Human
Thanks!

Lance Spitzner
Director, SANS Security Awareness
Email: lspitzner@sans.org
Twitter: @lspitzner

Two day course on building secure behaviors - securingthehuman.sans.org/events
Bob Smith  Cyber/IS Communication Specialist  
2 days ago  

We just had an incident recently reported to us by 2 different regions in our footprint. The employees stated an "auditor" had called them asking for organizational hierarchy information. Due to our education and awareness to our employees they were smart enough to not divulge any information to the caller and reported the incidents to us. We then put out an Information Security Alert letting others know about the social engineering (do not fall for this common trick).

In reply to Ispitzner

Betty Torrey @goatblockchain  
3 days ago  

We had a user report to the NOC that file extensions were changing to .zepto in a shared folder on a file server. This allowed us to stop the encryption and start to rebuild the server within 10 minutes of the initial infection. We all let her know she was a rockstar.

It was only due to a couple of people talking to each other and directly to their counterparts at the other end of the invoice, questioning it, and having one of the team put their hands up and say they thought they may have done something ill-advised, that we were able to understand what was happening, and work with the client to ensure that we didn't let funds get diverted. (In fact, I was logging calls with Action fraud, WHILE the woman was on the phone!)
We just had an incident recently reported to us by 2 different regions in our footprint. The employees stated an "auditor" had called them asking for organizational hierarchy information. Due to our education and awareness to our employees they were smart enough to not divulge any information to the caller and reported the incidents to us. We then put out an Information Security Alert letting others know about the social engineering attempt, what to look out for and reminded them the proper steps to take (do not give out info, report to us, etc.)
Security Awareness Maturity Model

- Compliance Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainment & Culture Change
- Metrics Framework
BJ Fogg Behavior Model
Key Behaviors – What to Teach?

- Clues of an Incident
- Reporting of an Incident
- Comfort with Reporting
Clues (not Indicators)

- Pop-up you computer is infected, pay ransom
- You clicked on a link and something bad happened
- Friends report getting odd emails from you
- Password no longer works even though you did not change it
How to Report

• People not only can explain process but demonstrate it.

• How many ways to report in your organization? Death by email alias?
Comfort in Reporting

- Do people feel comfortable reporting?
- Will they get in trouble?
- CEO video story
Summary

- We perceive people as being the weakest link when with some training, they could be your strongest sensor network.
- To create human sensors, you need a program to train them.