

SUPER USERS!

***TEN RAD WAYS YOU CAN HELP YOUR
USERS IMPROVE YOUR SECURITY***

Justin Hall, CBTS

Presented to the NKU Security Symposium

HELLO!

I'm Justin Hall.

I'm the Security Services director at CBTS.

Jesus follower, husband, dad, gamer, eater of pie.



DFWG

cbt

Users drive security people

CRAZY!!



**80% OF COMPANIES SAY
THAT "END USER
CARELESSNESS" IS THEIR
BIGGEST SECURITY THREAT**

KNOWB4/ITIC STUDY

WHAT IF...

Instead of being a **liability**, our
users were considered an

ASSET?!!



FIVE "DO'S"

(Most of these are for you to do, not your users)



1. **DO** *KNOW YOUR OWN DATA*

Classification

Understand the types of data you own, sort into categories, and set rules and policies for each category.

Communication

Tell your users what their responsibilities when handling your data. Provide a lot of examples.

2. **DO TALK TO THEM LIKE THEY'RE ADULTS**

- × Don't patronize
- × Talk about what's serious
- × Emphasize actions and consequences

3. *DO GIVE THEM INCENTIVES TO HELP*

- × Reward good behavior
- × Start a scoreboard
- × Keep things fresh

4. **DO TALK ABOUT ACTUAL ATTACKS**

- × Research the TTPs
- × Put yourself in the victim's shoes
- × Remember, "It can happen to us!"

5. *DO PHISH YOUR USERS*

People change their behavior more through experience than simply being told.

5. *DO PHISH YOUR USERS*



41% Click Rate
2014



15% Click Rate
2016

CBTS Phishing Assessment customer results



FIVE DON'TS

(Again, these are for you, pay attention)



1. ***DON'T OUTLAW NORMAL BEHAVIOR***

Sometimes, attackers do the same things normal users do.

Sometimes, you need to let users continue to do those things, and **monitor** for suspicious activity instead.

2. ***DON'T LET THEM GO WILD ON THE WEB***

- × You're responsible to protect the organization and your data.
- × It's your internet connection/computer, not theirs.
- × Use a content filtering proxy.

3. ***DON'T USE A CRAZY PASSWORD POLICY***

Discourage insane complexity.

Normal humans don't remember them, and the common attack vector (PTH) doesn't care if it's complex.

Encourage passphrases.

The uncommon attack vector (cracking/guessing) is defeated by length more than complexity. Plus, they're easier to remember.

4. ***DON'T LET USERS POSTPONE PATCHES***

They'll complain for a bit, and then get used to it.

(They might even be glad they don't have to turn their machine in as often to get it reimaged.)

5. ***DON'T CHEAP OUT ON AWARENESS***

Avoid:

- × Boring Powerpoint
- × “Watch this video of a thief piggybacking”
- × Stuff that’s not engaging
- × Super-technical lingo and processes

5. ***DON'T CHEAP OUT ON AWARENESS***

Focus on:

- × Video content normals actually want to watch
- × Clear, concise, actionable processes and recommendations
- × “We’re here to help! Call us anytime!”

SO, IN REVIEW, DO:

Know your own data

Talk to users like they're adults

Give them incentives to help

Talk about actual attacks

Phish your users

DO NOT:

Outlaw normal behavior

Let them go wild on the web

Use a crazy password policy

Let users postpone patches

Cheap out on awareness

THANKS!



Any questions?

justin.hall@cbts.net | cbts.net/security | @justinhall