

The Human Element in Election Security

Good Cybersecurity Practices for Election Offices and Campaigns



April 26, 2018



Clinton Campaign Hack

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.google.com/security> to do both. It is absolutely imperative that this is done ASAP.

Source: <https://mobile.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?referer=>



Human Beings Screw Up

You have to hack a computer, but you just have to ask a human.

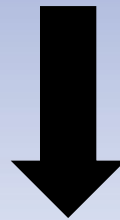


Obviously, computers and machines are still vulnerable.



Change Cybersecurity Culture

Knowledge



Attitude



Behavior



Knowledge

- What is a successful hack?
- The best defense is a good offense: If our office is on the defensive, we're already too late.
- Resources: SANS Securing the Human; News Articles; Non-profits



Attitude

- Everyone is a target
- Have healthy skepticism
- My email: `firstname.lastname@workplace.com`
- Removing the org. chart
- Dedicated phishing email address



Behavior

- Phishing Tests
- Cybersecurity checklist
- Two-factor authentication
- Principal of Least Privilege
- “Log Off Before You Walk Off”



Behavior

- Practice during the easier times
 - Table Top Exercises
 - CyberStorm VI
- Learn certain lessons now instead of on Election Day
 - Roles and responsibilities



Behavior

- Information control
 - MS-ISAC
 - “Employees of for-profit companies or non-profits, consultants, or private citizens that are unaffiliated with an eligible entity...”
 - EI-ISAC
 - Nat’l Cybersecurity Center



Behavior

- Not above shaming
 - Post It notes
 - Don't ruin this for the rest of us

