Goal	**Reduce Donors Affected by Leaks to Less than 1,000/Year**								**Goal**
Subgoals	**Prevent Access to Sensitive Information of Donors**				**Prevent Exploitation of Employee Privileges through Phishing Scams**				**Subgoals**
Behaviors	**Keep track** of where donor data is stored	**Restrict access** to donor data	**Identify legitimate reasons** to access data		**Do not provide credentials** to untrusted sources	**Do not run programs** from untrusted sources	**Report suspicious** emails for analysis	**Confirm unexpected** email requests by phone	**Behaviors**
Practice	Find everywhere donor names are stored	Prevent access to donor data from everyone for 24 hours	State whether given purpose is legitimate and why		Do not provide credentials in a page opened from email link	Do not open an executable file attachmed to an email		Call by phone the colleague who requested donor details by email	**Practice**
Practice	Find everywhere donor emails are stored	Allow specific employees to access donor data	Propose an alternative to access less sensitive data		State whether a URL is hosted on the Intranet or on the Web	Deny request to run an unexpected program		Call by phone the manager who requested a wire transfer by email	**Practice**
Practice	Find everywhere payment info is stored				Compare the URL in an email with the URL of the target page	Do not follow instructions from email to alter settings			**Practice**
Information	Where donor data is stored with all copies	Who needs access to donor data	What is donor data regularly used for			Which kind of files may run on a computer	Where to forward emails for analysis		**Information**