Guidance for Protecting Personal Information Online

One tactic employed by animal research opponents (extremists) is the targeting of individual staff members through personal emails, home addresses or their social media accounts. Because this is the case, it is often a good idea to regularly remind both new and longtime staff of steps they can take to better protect personal information from these types of harassment.

| Social Media Security | Networking and producing content online about your personal experiences and opinions is a matter of daily life for so many individuals. It is up to the individual to assess their own comfort with the risks that accompany posting online. We should point out that a growing trend is extremists targeting employees via social media. Typically, extremists use the approach to pressure individual scientists or research facility leadership. However, groups have also been known to gather and use information they have obtained from employees at all levels of an organization who share their experiences and observations online. With that in mind, here are a few tips:  
  
  - One good way to avoid harassment or misuse of your information is to be mindful that once something is placed online, it can end up anywhere. There have been countless instances where screenshots of private messages, social media posts or texts have been shared with a much broader audience than intended. Think before hitting send about how certain statements might be misunderstood or misused by others with an agenda. If you have concerns, don’t share it. Think twice before you tag people and then associate them online to keywords/# or physical locations. In many cases, employees post messages that feel benign to them because they were written for a very specific audience. Consider phone calls or in-person discussions with peers about sensitive topics. Other communication platforms may be well-suited for these types of exchanges.  
  
  - It’s recommended to occasionally review your privacy settings. Consider limiting communications - or perhaps certain types of communications - to very close acquaintances.  
  
  - If you turn to social media to share typical daily work frustrations, consider alternate outlets. Perhaps there are better social structures for blowing off steam or having |
healthy discussions about ways that work can be improved.

- It’s recommended that you review your own social media profiles. You may wish to list just our host university instead of your specific research unit. Think about whether you are comfortable with including your official job title. Tip: View your social media profiles links using “Incognito” or the “InPrivate” mode on a web browser to see what information is publicly available.
- It is possible to search Facebook for mentions (ex. @yourname) of your name. However, because Facebook posts are not indexed by Google and other leading search engines, you can only search within Facebook.com.
- Staff might consider making their Facebook “friend” list NOT viewable to the public and/or making their social media accounts viewable only to approved friends or followers. This might prevent friends or family becoming targets from unwanted messages. Additionally, when friend lists are visible to anyone, there have been cases of fake social media accounts made with the same photo of an existing friend. A new friend request is then sent, leading someone to think they somehow “lost” the friend and need to re-add them. In fact, they are adding a fake profile to their friend list.

Another option is to talk with your media relations office. Some press offices have even more powerful software that can be used to search for certain names and terms. In some cases, they may be able to set up searches for staff and admins who are at high risk and alert you if something shows up.

<table>
<thead>
<tr>
<th>Records Requests:</th>
<th>Make Certain Information That Can Be Protected, Is Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>At times, staff contact information, including cell numbers and email addresses, is included in information requested through FOIA or state records requests. Talk with your legal office to make sure this information is protected whenever possible.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What to Do if You Receive a Concerning Email or Call</th>
<th>If you have already received an email, letter or call from an animal rights extremist or group, here are some things you can and should do.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- When an unwanted communication from an extremist arrives, it should be routed through the Director’s office (and may also be escalated to the University Police Department. This is</td>
<td></td>
</tr>
</tbody>
</table>
crucial when the message is threatening in nature. But we believe security should be looped in in all cases.

- One option is to **do some online detective work** to see if you can determine how your data was obtained. We’re of course, not suggesting that you ask the person who contacted you where they obtained your information. But sometimes, a quick web search will reveal the source. Unfortunately, there are several affordable services that extremists can easily use to obtain personal information gleaned from utility or election records. Security or communications staff may be able to assist with some of this detective work to curtail future problems.

<table>
<thead>
<tr>
<th><strong>What to Do if You Receive a Letter</strong></th>
<th>You may choose to send junk mail back by leaving the envelope unopened, and writing “Return to Sender” on it before dropping it back in the mail. Scratching out any barcode or routing information is encouraged in order to prevent the piece of mail from being automatically sorted and delivered back to you in error. You don’t need to put any postage on the envelope since the post office will return it to the company who sent it.</th>
</tr>
</thead>
</table>

| **Protecting Personal Online Data** | One good strategy for determining your personal level of risk is to conduct occasional web searches to learn what is out there. Try searching your name along with other keywords and phrases such as “animal” “research” and “animal research.” You may also want to search for your name along with the kinds of animals you work with. **Tip:** Search your name in quotes (Ex: “Joe Wilson”) for better results. If you find anything concerning, take action if possible. Those steps might include:  
  - Updating your LinkedIn profile or other social media profiles.  
  - Asking your current employer to address issues with your online profile.  
  - Asking a former employer to remove your information.  
  - Contacting a company that you have done business with and asking them to remove your personal information from their website.  
  - Making adjustments to personal webpages or blogs to protect information and only share these pages with friends and family.  
  - Don’t forget to check what may be listed in any online university or company directories. It’s believed animal rights groups are increasingly using these directories to target staff |
|--------------------------------------|--------------------------------------------------------------------------------------------------|
with emails, calls and letters.

- In extreme cases, where harassment is already taking place, some may wish to change personal email addresses, or initiate a new primary home email account.

### Monitoring for New Content

One good strategy for learning when new information is posted about you is to set up one or more Google Alerts (www.google.com/alerts). This free service allows you to setup regular searches for keywords or phrases. You then receive alerts via email or RSS (your choice) when those terms newly appear online. Here are a few tips for setting up effective Google Alert searches:

- Place your name in quotes to help narrow results. If you have a common name, consider adding additional terms (Example: “Joe Wilson” and “animal” or the name of your university or lab.)
- If you like, you can set up a Google Alert that will let you know when your personal email address is newly posted online.
- You may want to set up alerts for variations on your name (Example: “JoeWilson” and “Joseph Wilson.”)
- You may also want to set up a separate search for your company or university name. Again, consider adding additional keywords to focus results to avoid getting overwhelmed with lengthy alert email.
- **Note:** There are many websites used to find people on the internet. We encourage individuals concerned with their information being listed on these sites to follow the instructions for having that info removed. These are some examples of those websites: Intelius, Pipl People Search, Google Groups, TruePeopleSearch, FindPeopleSearch, PeekYou, Classmates, FamilyTreeNow, TinEye, ZabaSearch, US Search, Linkedin, and Facebook.