Awareness: An Anti-virus Program for Humans

Gretchen Morris, CISSP

DB Consulting Group, Inc.

Integrated Awareness Efforts

- Website
- News Articles
- Security Tips
- Calendar(s)
- Newsletters
- Posters
- Webinars
- Lunch and Learns
- Blogs
- Online courses
- Books
- Videos
- Training Catalog…

Website

- Main communication tool for your team
- Post (list) all other awareness activities here
- Have each of them point back to your website

Point to other helpful websites

- FTC https://www.ftc.gov/
- Stop.Think.Connect https://www.dhs.gov/stopthinkconnect

News Articles

- NSI – Security Sense (vendor Provided) or internally created
- Current issues and concerns
- Post to website
- Use to create Security Tips, Include in newsletter

Caution! Emails You Should Never Open

March 3, 2016

Despite the best efforts of security researchers, too many people are still falling prey to email scams. Whether it's a get-rich-quick scheme or a sophisticated spearphishing attack, here are some emails to steer clear of:

1. **The government scam.** These emails are made to look as if they come from government agencies, such as the IRS, FBI, or CIA. Believe us, if they want to get a hold of you, it won't be through email.

2. **The "long lost friend."** This scammer tries to make you think you know them, but might also be a contact of yours that was hacked.

3. **The billing issue.** These emails typically come in the form of legitimate-looking communications. If you catch one of these, log into your member account on the website or call the call center.

4. **The expiration date.** A company claims your account is about to expire, and you must sign in to keep your data. Again, sign in directly to the member website instead of clicking a link in the email.

5. **You're infected.** A message claims you're infected with a virus. Simple fix: Just run your antivirus and check.

6. **You've won.** Claims you won a contest you never entered. You're not that lucky; delete it.

7. **The bank notification.** An email claiming some type of deposit or withdrawal. Give the bank a call to be safe.

8. **Playing the victim.** These emails make you out to be the bad guy and claim you hurt them in some way. Ignore.

9. **The security check.** A very common phishing scam where a company just wants you to "verify your account." Companies almost never ask you to do this via email.

Security Tips

Cyber Security Tip

Despite the best efforts of security researchers, too many people are still falling prey to email scams. Whether it's a get-rich-quick scheme or a sophisticated spearphishing attack, there are some emails you should steer clear of. Read the SECURITYsense article, "Caution! Emails You Should Never Open," to learn more.

URL: https://your.website.gov/2016/caution-emails-never-open/

- Create from News Articles
- Post to the website and your organizational internal news page
- Can also Include in
  - A monthly printed calendar
  - A newsletter

Calendar

- Annual calendar
- Topics feed into Newsletter article selection
- Topics feed into Webinar topic and speaker selection
- List rules of behavior or other important information on the back
- Post to website

Privacy of Information

Data Privacy Day, held annually on January 28, encourages everyone to make the protection of privacy and data a greater priority in their lives. Everyone needs to be aware of the personal and private data others have entrusted to us and remain vigilant and proactive about protecting it.

January 2015

S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Spam & Phishing

Spam and phishing are not limited to just email. They are also prevalent on social networking sites. The same rules apply on social networks. When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts.

February 2015

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Securing Your Home Computer

To protect your home network you need to have the right tools in place and confidence that family members can use the Internet safely and securely. The first step is to make sure all of your Internet-enabled devices have the latest operating system, web browsers and security software.

March 2015

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Telework

Telework refers to the ability to work from anywhere. Be sure you review security and privacy policies to ensure that security and confidentiality are maintained at all times.

April 2015

S	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Social Media & Passwords

Social media is an integral part of our online lives. Information Technology allows us to stay connected with others, but there are risks. Take the time to review and adjust privacy settings to protect your personal data and postings.

May 2015

S	M	T	W	Th	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

National Internet Safety Month

June has been designated as National Internet Safety Month to help raise awareness about staying safe online, learn about cyber security issues that we face today and know what tools are available to protect your personal information.

June 2015

S	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Mobile Devices & BOYD

Take the same precautions with your mobile devices as you do your computer. Using a mobile device to access NASA resources must be done securely and must meet and maintain a minimum set of security requirements.

July 2015

S	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Malware

Malware, short for malicious software, is any software designed specifically to damage or disrupt computer operation, gather sensitive information, or gain access to a computer system. Criminals use malware to steal personal information, send spam, and commit fraud.

August 2015

S	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Cyberbullying

Cyberbullying is the use of electronic technology to harm or harass other people in a deliberate, repetitive, and hostile manner. Every age group is vulnerable to cyberbullying, but teenagers and young adults are common victims.

September 2015

S	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

National Cyber Security Awareness

National Cyber Security Awareness Month (NCSAM), held every October, is an annual cyber security awareness-raising effort. Cyber security is our shared responsibility and that means everyone has the potential to make a difference.

October 2015

S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Online Transactions

Online transactions offer convenience if accounts are secure. For all online accounts, choose a different password containing upper and lower case letters, numbers, and special characters.

November 2015

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Identity Theft

Identity theft is a term that refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

December 2015

S	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

For additional information and tips, visit the IT Security Awareness and Training Center
https://your.websiite.gov/itsatc/

Another Calendar

- Monthly calendar
- All training events listed on the dates they occur
- Other important dates listed also

February Training Schedule

- **Risk Management**
  2/4 - 2/5 (9AM - 4PM) Room B322
- **Security and the Role of the COR/GTL**
  2/6 (9AM - 5PM) Room B322
- **CMS ISSO Training**
  2/18 - 2/20 (9AM - 5PM) Room B310
- **SCoE Meeting**
  2/20 (12PM - 2PM) Room C112
- **ISSO Monthly Meeting**
  2/26 (1PM - 2:00PM) Room C114

Security Tip of the Month

Recognizing and Avoiding Spyware

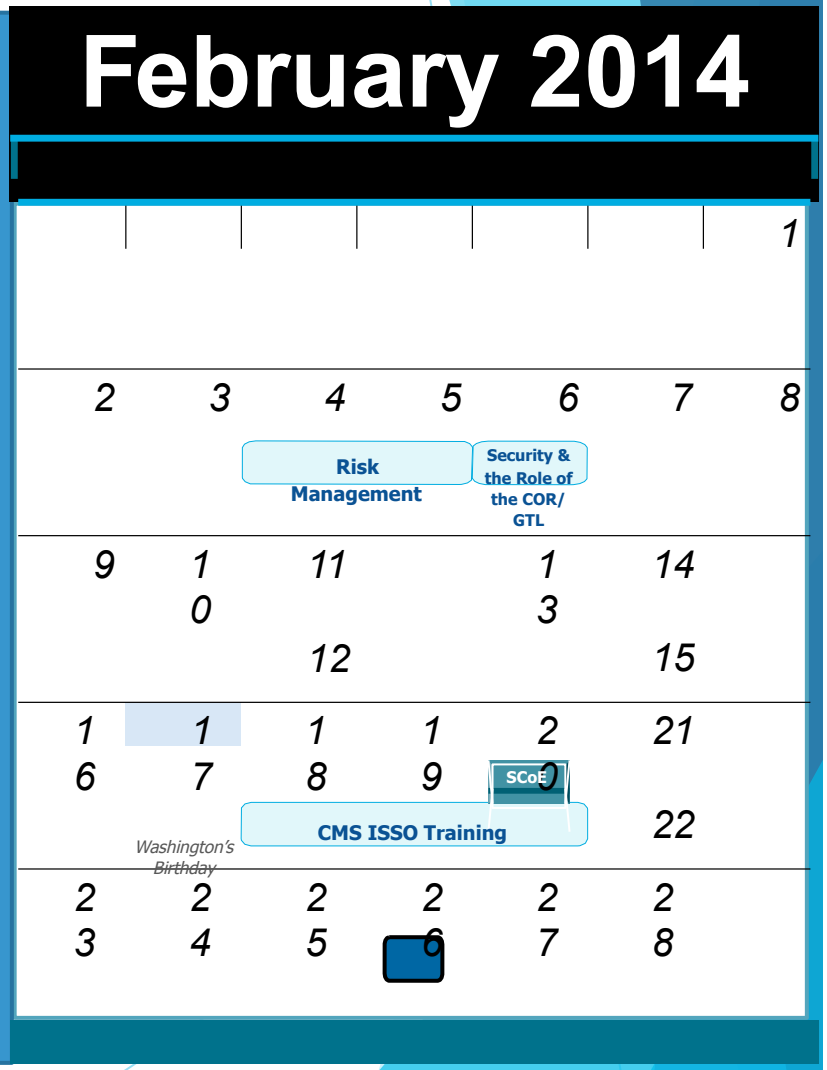
The following symptoms may indicate that spyware is installed on your computer

- ⇒ you are subjected to endless pop-up windows
- ⇒ you are redirected to web sites other than the one you typed into your browser
- ⇒ new, unexpected toolbars appear in your web browser
- ⇒ new, unexpected icons appear in the task tray at the bottom of your screen
- ⇒ random Windows error messages begin to appear
- ⇒ your computer suddenly seems very slow

To avoid unintentionally installing it yourself, follow these good security practices

- ⇒ Don't click on links within pop-up windows
- ⇒ Choose no when asked unexpected questions
- ⇒ Be wary of free downloadable software
- ⇒ Don't follow email links claiming to offer anti spyware software

Reference: http://www.us-cert.gov/ncas/tips/ST04-016



Newsletter

- Quarterly, Monthly, Semi-annually
- Include
  - “Easter eggs”
  - Interviews
  - Security cartoons

May 2014 Issue 12

INFORMATION TECHNOLOGY DEFENDER

From the OIMT Information Security Program

Inside this issue:

1-2 Is There Such a Thing as Privacy on the Internet?

2 Guidance on Use of Unauthorized External Systems to Conduct Government Business

3 FDA Wins at FISSEA

3 CDRH Organizational Awareness Day

Report an Incident

If you suspect lost, misplaced or stolen equipment, or a breach of Personally Identifiable Information (PII), notify your equipment manager **AND** contact the FDA Computer Security Incident Response Team (CSIRT) at:

- **Email: SecurityOperationsandResponse@fda.hhs.gov** or
- **Toll Free Number:** 855-5FDA-SOC (855-533-2762) (24x7)

Is There Such a Thing as Privacy on the Internet?

Have you ever Googled yourself?

If you have, you might find a lot more than you bargained for. It is increasingly difficult to remain anonymous on the internet. A lot of the information you'll find on yourself online is already considered public information. For instance, when you buy a house, details of the transaction are recorded in the local courthouse, to include the purchase price and the names of the buyers and sellers.

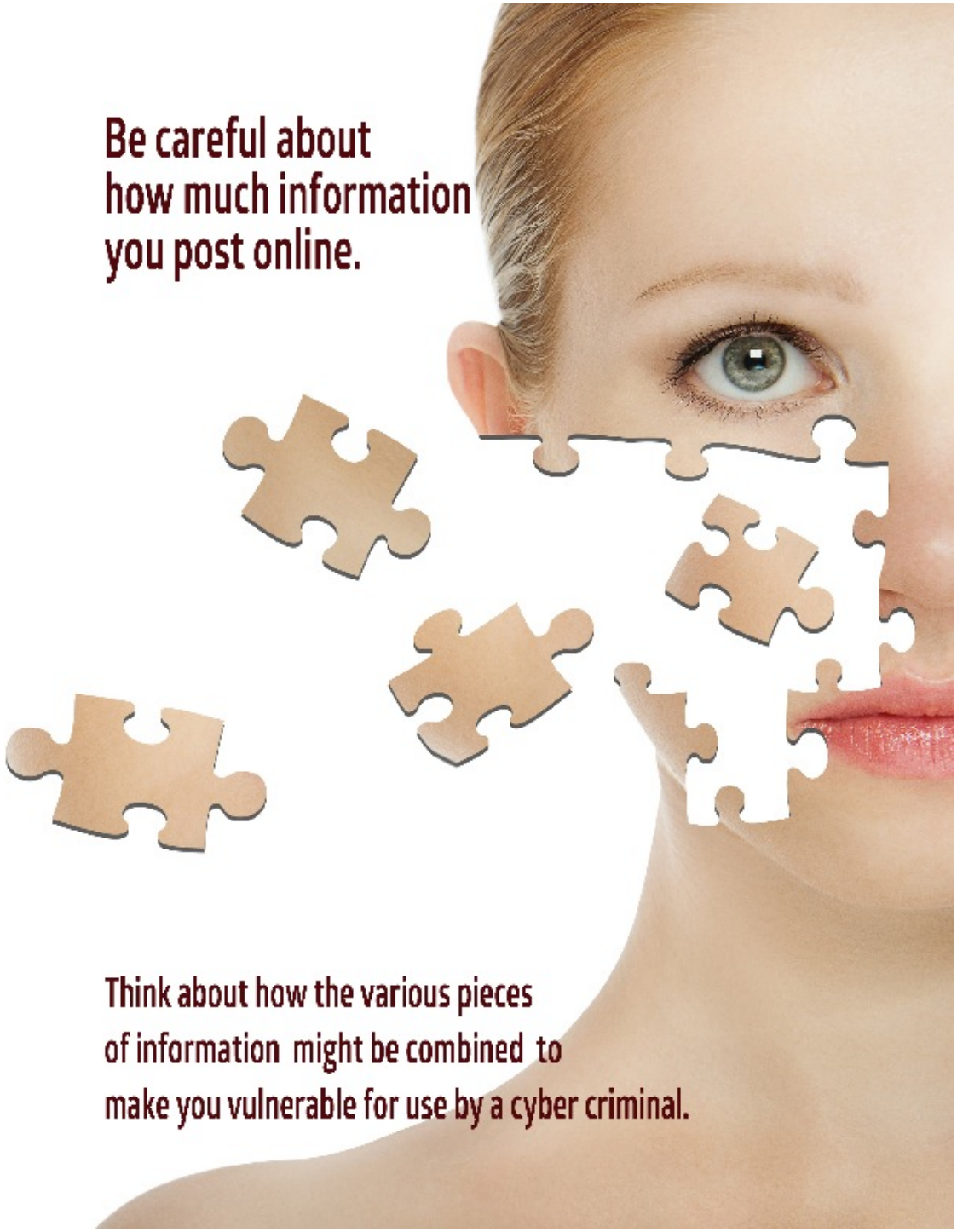
It has become much easier to collect information about an individual by collecting public information and personal data you publish on social media sites (Facebook, Twitter, etc.). While there are certain things that will always be part of the public record (such as home sales), there are some things you can do to reduce your “digital footprint.”

Helpful Tips to Reduce Your Digital Footprint:

- If you are a Facebook user, make

Posters

- Monthly, quarterly
- Tie in with calendar themes
- Cover current Incident Response Management concerns
- Keep them simple (uncluttered)



Webinars

- Cover current topics of interest
- Follow monthly theme
- Offer technical and awareness topics
- Allow the learners to use webinar functionality (like chat for questions)
- Allow for interaction (Q & A) with the speaker

WEBINAR COUNTS AS 1 CPE

IT Security Awareness & Training Center

CYBER SECURITY WEBINAR

TOPIC: Social Networking
DATE: Thursday, February 25, 2016
TIME: 2:00 – 3:30pm Eastern
1:00 – 2:30pm Central
11:00 – 12:30pm Pacific

The focus of this webinar will be to examine the intrinsic nature of social networks and the impact to users. Mr. Willis's presentation will highlight popular social networking sites and the most frequent scams and risks associated with user participation.

Takeaways:
- Resources that enable users to stay current on social networking risks
- Tips to easily recognize social networking scams
- Increase your understanding of new terms associated with risks such as "Like Farming"
- A more in-depth understanding of "how" bad guys collect personal information for the purpose of hijacking your accounts, and accessing other identity information

FEATURING:
Carl D. Willis-Ford,
Solution Architect, CSRA

Carl Willis-Ford started his career as a Nuclear Reactor Operator on fast attack submarines in the U.S. Navy. Post-Navy, he worked as a Federal Civilian Manager at Puget Sound Naval Shipyard until joining SRA (now CSRA) in 1997, where he currently works as a Senior Solution Architect. In 2013, he received the SRA Individual Excellence Award and was also named a Senior Member of the Information Systems Security Association. Willis-Ford is also a member of the Board of the Federal Information Systems Security Educators' Association (FISSEA).

He holds a B.S. in Computer Science, an M.S. in Network Security, an M.S. in Technology Management, and is currently pursuing a doctorate in Information Assurance at the University of Fairfax, where he is researching user compliance, training & awareness, and security governance.

To Register:

Log into SATERN and search for ITS- in the catalog. Select the Cyber Security Webinar entry. Select the register tab. Make sure to confirm registration. Questions? Contact: ITSATC@lists .gov

Lunch and Learn

- **Open lines of communication** between IT Security and the employees
- Allow IT Security to share information in an **informal environment**
- Allow the employees an **opportunity to discuss** activities and ask questions regarding IT Security

Blogs

- For you
  - Training trends: http://elearningbrothers.com/20-elearning-blogs-you-simply-have-to-bookmark/
  - Current security issues: http://krebsonsecurity.com/
- For everyone
  - https://staysafeonline.org/blog/
- Post to your website, list in your training catalog

Online Courses

- On your Agency LMS
- Hosted by other vendors
- Freely available courses
  - Fed VTE
  - Other Agencies

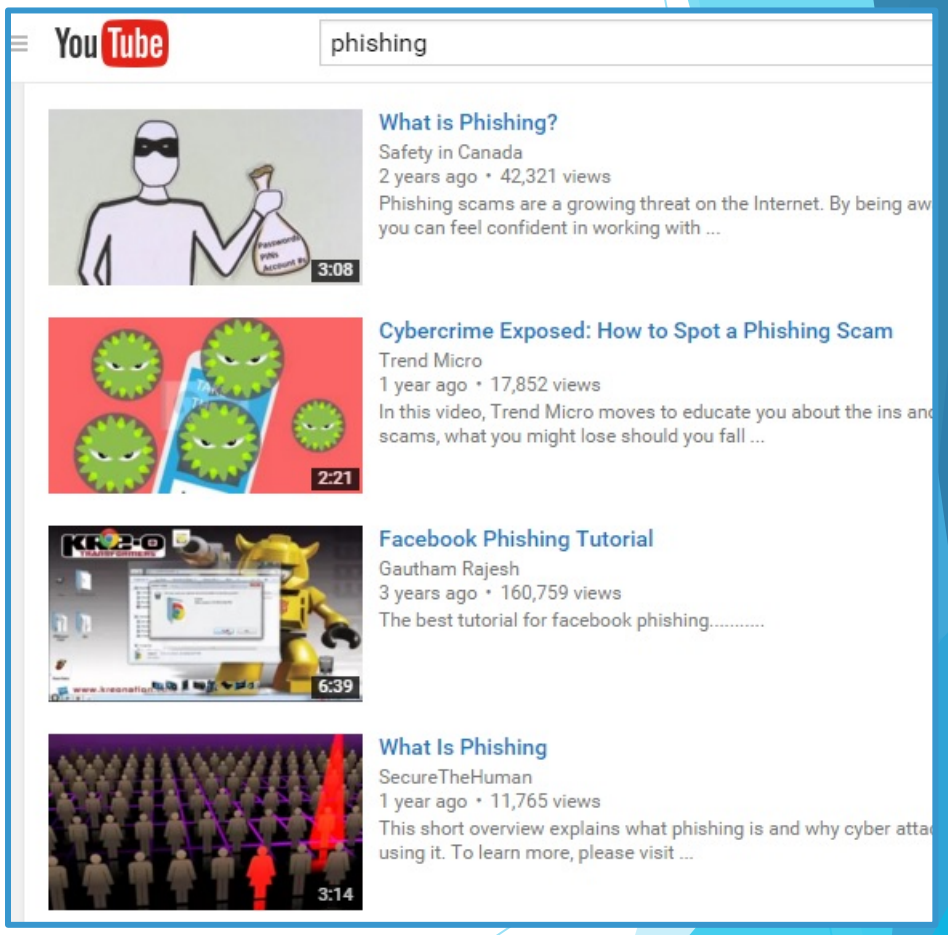
Books

- Set up categories according to areas of interest
- Advertise on how to access
- Some have the ability to have chapters downloaded to mobile devices

Personal (Home) System Security	
	The Essential Guide to Home Computer Security
	Mobile Device Security for Dummies
	Simple Computer Security: Disinfect Your PC
	Simple Computer Transfer and Backup: Don't Lose your Music and Photos

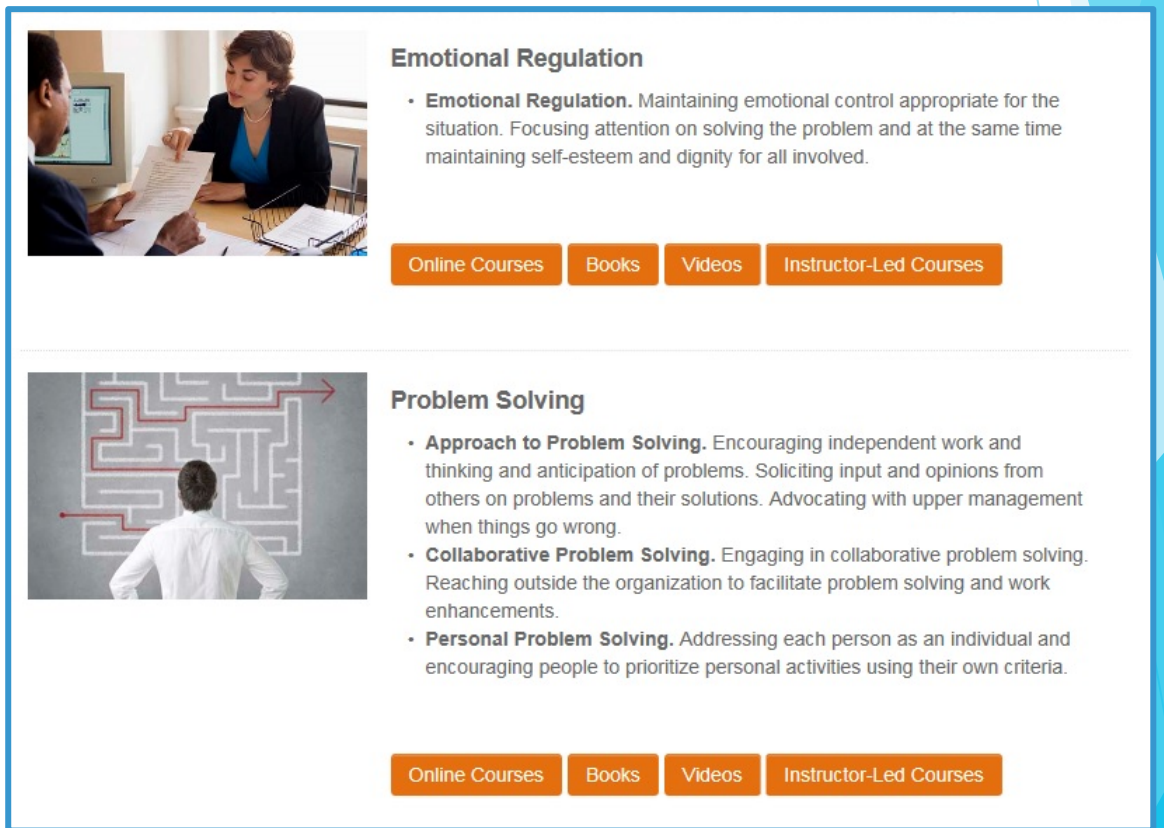
Videos

- Locate and advertise
- Create if you can
- Point to them from
  - Newsletter
  - Security tips
  - Online courses
  - Website
  - Course catalog

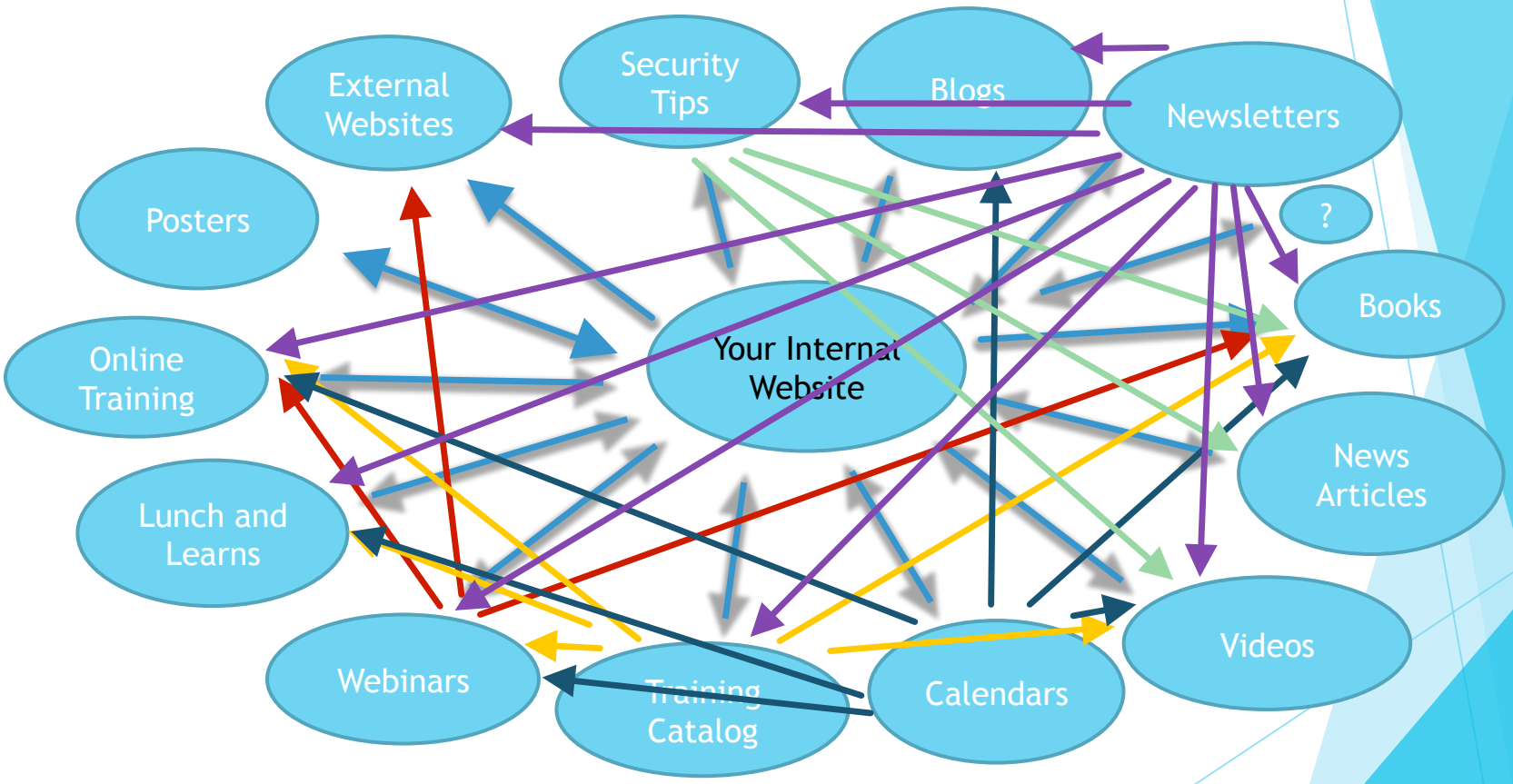


Training Catalog

- Print and share
- Make it available online
- Include a list of all that may be helpful or available to different audiences



How it all “fits” together



For Your Technical Learners

- Examples:
  - Internal security alert listserv that bundles many of the common alerts.
  - List of external websites that list security concerns and alerts.
  - Technical webinars with experts to help them learn more about a topic and give them an opportunity to ask questions

Questions?