

2015 FISSA+ Course Survey Comments

What about this class was most useful to you?

This is the 10th time I have taken this training at least. I spend a lot of time on computers both at home and work. I build my own home computers so I am up to speed on vulnerabilities. I am pretty diligent on behaviors that lead to problems. Over the years this training has helped remind me to stay that way.

Not much. I've taken this training so many times I pretty much know it by heart.

The explanation of two-step verification provided greater insight into why our Department required the move to PIV cards, which has been, heretofore, inexplicable.

I've taken this course ever since it was instituted (I've 30+ years government employment) so nothing new was presented this year. It was just a reminder.

Info in the last module about the newest online threats. Though it would have been really nice to have learned some ways to counter them, not to just be freaked out and almost too paranoid to go online anymore.

You are making it to complex the only thing we need is common sense and you can't teach that

New and updated information, much better than prior versions of the class.

I am a long time employee that has had to take this training every year. This year's course was the best. It was written and organized for a lay person without much knowledge of the course material. This made it easier to read and to take the training.

Combining all the annual required training into one class was a stroke of genius.

I find the course was extremely well prepared and an effective tool for users. I tested all links which all were functional. Well structured.

It was to the point; the test was on the material that you just read and to the point. It was compacted, easy to read and get through, really enjoyed it this year, very well done.

What about this class was least useful to you?

The graphic user interface is too demanding on bandwidth for remote National Park Service locations. We need a low-bandwidth option.

Module 3, slide 4 of 25 has an error: Casinos know their average daily payout. (The most generous casinos allow gamblers to win 2% of money wagered.) This whole slide is somewhat kooky. Profit shouldn't be the main concern with respect to risk, and especially not for Federal agencies, which by definition are non-profit. Damage to an organization's reputation and public trust is hard to quantify in terms of dollars, and I believe it's not important to our understanding of risk to frame all losses in terms of

dollars. (a very limiting view). Module 3, slide 6 "Since humans will always make errors, the risk from unintentional threats is 100%." I'm pretty sure that I have at least a few error-free moments each day, so my risk from unintentional threats is not 100%. "Examples of unintentional threats include losing a thumb drive, a laptop or other mobile device, or accidentally deleting or overwriting data. The vulnerability is human fallibility, the likelihood is certain, the frequency is daily, and the impact of data lost could be minimal to extreme over a period of a day." This is another dumb statement. The risk can only be 100% if 100% of the events result in a loss. I'd have to lose my thumb drive every time I use it for the risk to be 100%. We'd have to lose 100% of our data by overwriting it every day for the risk to be 100%. I'm concerned that the developers of Module 3 don't have an adequate understanding of the content or their target audience. The statement "Every day, someone in DOI accidentally deletes a file, unintentionally changes data in databases, or loses a device" has not been proven. Overstating is bad form. "Every day, someone in DOI accidentally deletes a file, unintentionally changes data in databases, or loses a device. Although it is a certainty that someone somewhere will unintentionally compromise data, we do not stop using computers because there is a 100% risk of data loss." Oh brother, another dumb statement. I'm sure that the DOI has not lost 100% of its data. The content developers need to revisit this section.

The modules required nearly constant re-launching the training program. Example: I'd get to the 22nd slide or so (22 of 25 or similar), then the "next" button would disappear and I'd have to re-launch and click back to where I was. This even happened during one of the tests. Very aggravating. Had to re-launch the program over 10-times. Others in my office were aggravated by the same thing.

Finicky computer delivery system. Computer locked up 9 times and had to relaunch.

The class required refreshing the screen 8 times in the first segment and then I lost connectivity completely in the first test. Our infrastructure just doesn't support this type of training.

Wireless security. We are not allowed wireless technology. I had several technical problems during the training. Once I clicked to take a test and was thrown out of the program and 3 times the program froze when no "next" button appeared and I had to exit and work my way through the module again. Very frustrating and distracting. Even getting into DOI Learn is made difficult because my password never works and I have to get a new one.

Initial information regarding this course/class tells me that I should be able to complete it in an hour and a half or something like that. However, in order for me to remember what I have read/learned and because there is so much of it to review without a break, I sometimes have to reread part of the class. Also, because I am interrupted and have to leave the program to return later to complete a segment, I have to re-familiarize myself with parts of the course. So what's my point? Competitive folks with a full plate like myself have to constantly remind ourselves that it isn't necessary to complete this program in 1.5 hours. It is the retention of knowledge and the knowledge in its application that is foremost, and not the speed within which we must complete this course.

You need happier sounding audio. not so melonically, monotones are kinda depressing

The method of delivery. For the second year in a row the system constantly stopped working. At random times the "Next" button would disappear forcing me to exit the system and restart the class. I had to restart the class more than 20 times. About half the time the program would not reload and I had to exit again. When the course did load, it only worked through a partial lesson. It took me more than three hours to complete. This was a complete waste of my time. Again, this problem is the same from last year.

The user interface was terrible. It continually locked up! It required 8 tries to complete, using both chrome and IE. If it were not required, I would have given up taking the course much sooner!

it was all relevant new information for me ****when I tried to go to an example e.g. a handbook I was kicked off the site and had to start over/ it was hard getting more indepth information because of this

The length of time it took to complete the course. It took me over 6 hours & 13 attempts because of it continually crashing, it said to use internet explorer but it was slow in loading, so I used firefox--which went smoother and faster.

Don't put images behind the text. It makes the text difficult to read.

I was disturbed by the fact that I had to complete the course twice (all 5 modules and related tests) to get a certificate. Apparently, after completing the course and getting a 97%, the system did not save my results and in order to get a certificate I was forced to redo modules 2 to 5. Thus, the course can be more useful if I can successfully complete it in the least time possible.

I hated trying to get into the class. It took me over 15 tries to finish the class due to not using internet explorer. It should of been red flagged more and supervisors informed that it was okay to use internet explorer. We were told last year due to security problems to not use internet explorer or else!!!

I could not download or open any tabs (glossary etc) because I would be shutout from the course and have to start again. I had to start many many times. I initially took this course at home and lost one solid day of productive work due to the connectivity of the course. Very dissapointed because of lost time and the frustration of trying to complete the course.

The constant being kicked off for no apparent reason!

Absolute waste of time. I click through as fast as possible (limited by screen refresh rate) and take the test. Always pass with 90+% on first try, which means the training / testing is worthless. The only reason for this training is to check a box in some managers EPAP and for the legal department. It also is a complete waste of taxpayer's money.

The background material, although likely useful, kicked one out of the training session necessitating getting back into the system - a real time waster. Therefore, the

background material went unread. To improve this and other training, make sure that links to background info does not kick one out - make it easier to get back to the training material and it will be more useful and likely read more.

For me it is two-fold. The repeating of content that deals with behaviors that I would never do. The other is how this training affects my employees who are less knowledgeable about the way networked systems work. The training can cause such fear that they lose productivity. They simply can't grasp the concept how to recognize the differences between socially engineered manipulation and work related links. They always end up coming to me to ask.

It got very technical for me to understand the terms and concepts with new malware ability.

This is the same information we get every year. To make it more relevant this should be a training update with any new threats, specific events, or new or updated laws that apply. This should not be a mandatory course every year. Also the course shut down near the end of each module causing me to have to exit the course and re-enter the course in order to finish. This even happened on one of the tests causing me to fail the test and I actually had to retake it. The program was so bad that it detracted from the content and made me want to proceed right to the shut down part so I could get it over with.

The long introduction to what we were learning.

Often, when I checked a link, e.g. example or resource, and tried to return to the training module syllabus, I was kicked off and had to return through DOI Learn. I was annoyed at the frequency of this occurrence, to the point of not checking the links unless absolutely necessary.

I missed a couple questions. One was about the distinction between http: and https: protocols. That concept could have been explained in more detail. Then, when I tried to go back and review that unit, the navigation was difficult. I had to start at the beginning and hit "next" until I got to the material I needed in the very last unit.

Wanted to get a copy of course but could only copy a page at a time

Multiple times, the NEXT button disappeared as I was going through the course. I had to close out of DOI Learn and log back in.... after multiple tries, the NEXT button would finally be there. This made taking this online course very frustrating.

I could not open or print most of the summary pages. The NEXT button was not appearing on several screens to advance the course. I had to re-login several times. The delivery of this course is not quite working properly.

We take the same training EVERY YEAR. Not much changes. Total waste of time. Please, please, please respect, at some point, that we can learn and retain this information for more than 12 months. Also, the software crashed 4 different times while I was taking the course, forcing me to go out and back in. Luckily the program was modified this year (it has done this for years...) to accommodate the flaws in the

software. It somehow feel disrespectful to have a broken piece of software unleashed on 25,000 employees.

Sentences that are filled with abbreviations do not communicate information well, for example, At DOI, the CIO for the Department is the SAOP and the DOI ISE Privacy Official.

The interface was really poor. Text from one screen would stay on the screen while more pages loaded.

When I opened linked items (i.e.: Rules of Behavior) I could not get back to the training and had to get all the way out and Launch the training again from DOI Learn. Very frustrating after a couple instances.

Not a clear path from extra files back to the training without being booted from the system.

I know the material. I scored 100%. I tried to skip through and take the tests, but the program hung and I had to reload it three times to complete it. It's a waste of my time. Unfortunately, it's a federally mandated waste of my time. Fix the d**n program so it doesn't lock up!

Unable to read the small print -- DOI Learn apparently still thinks that DOI employees still use 1990s-era monitors and who ever contracts out the course material has the compiler set the course material at a ridiculous resolution -- so I am unable to pull up a full screen version that is at least more readable than what is presented.

Some of the lead-in slides could be edited down a bit. Some were too wordy and it took a while to settle in and get my mind focused on the training. Also, it took me about 3.5 hours to do the course, and it got stuck at one point and I had to reload the course to continue.

How can we improve the training to make it more relevant to your job?

There are no participant materials (manual, presentation handouts, job aids, etc.). If I wanted to save a screen, I'd have to take a screen shot, manipulate it, then save it.

make it shorter, It takes over 4 hours to complete on the computer and half the time the system crashes and I had to start over. so shorten it up and stop the madness.

More examples of where security failed and consequences of lax security.

I'm not really sure you can. Improving and maintaining online security is reliant on all employees participating, yet some people are either too lazy to log out of their computers when they walk away from them, or they are too trusting, believing everyone within the walls of our secured facility are benign. It is difficult to see the value in completing this required training annually when compliance is not 100%. Similarly, I think it's easy for most employees to gloss over the content of the training because it is such an ordeal to get through each year. While I think online training is probably cost efficient, I think you would do well to occasionally require in person computer security

training so that your staff could understand how disengaged most people are with the annual FISSA training.

Write in English, not lawyer-speak. Use examples relevant to front line level people. MAKE IT SHORTER. Change the tone--it's so formal and stiff. If we all have to do this, why not make it clever and interesting? The visuals were awful and look like stock images that a bored middle school student pulled off the web. Seriously, our agency pays for sucky quality like that? Greater consistency (number of pages) between units would be appreciated.

It would help to be more system specific, or example specific where able. For example; tell me what I cannot do and what I can do. Sometimes this training leaves me with more questions and feeling unsure of what I cannot do.

85- 90 percent of employees, which is probably on the low side, already have this knowledge. Being a BLM employee for the last 4 years and a federal employee for the last 12 years, there have always been this type of training since I began my career. While it is great information, after the 2nd year of being a federal employee this information becomes common sense. Furthermore, anyone with an Associates Degree or higher already will contain this knowledge and if anything should receive this training when first hired. Another problem is that there is a test that determines the individual's final knowledge for a chapter or a final test for the training that has all of the same questions, which are usually in the same order for each individual. Each individual should have a random choice of questions and in different order so employee's will pay closer attention to the training and retaining the information provided.

Delivery of material was very technical and structured in a way that made it intimidating to learner. Either employees are at risk of compromising security of U.S. Gov or face imprisonment for violations they may not be aware they are committing. Need to tone down intimidation and provide more examples of how DOI Implements laws and policies.

The use of "watermarks" made some pages difficult to read

The first module is heavy on the different federal guidance--laws and authorities. Not sure if there is a better, i.e., more effective way of presenting them.

Some of the graphics in the backgrounds made it kind of difficult to read the text.

Please make the type easier to read by not putting watermark graphics behind the text. it's distracting and makes it harder to read. Also, it disturbing to have the paragraph text go all the way across the page that cannot be adjusted. The eyes need a rest and we can read faster when a sentence is not 7 inches long

The male speaker is so monotone he almost puts one to sleep!!!

Make so I don't have to mute each slide individually. I hate the audio of the text. I can read much faster then listen. Make the mute last through the whole presentation... I understand the audio needs to be there for ada compliance, but I am not blind.

It was pretty relevant to my job as it is. Maybe more about bison connect?

At least mention school use or use in an education setting.

Include less text about the laws, regulations, and policies.

For me? Make it more difficult. Make it a game where you try to thwart the criminals trying to break into my network system. Test me during the year with faulty emails and traps. Notify me if I screw up.

Make the presentation more interesting to listen to. Perhaps with "people" in the screens like you were listening to a real person for some of it.

Some of the voices performing the talking are a little monotone.

Please provide more information how to protect ourselves from identity theft from different social sites. Basically most of us are using different social sites at home but once our Identity is stolen, our job is at risk as well.

Maybe a short hands on class on how to secure emails and data devices. i.e. Such as traveling with Laptops, iPhone, etc. and securing these types of communication device.

Few people - probably none - in my office carry sensitive material around on portable devices. So that does not need to be emphasized as much. But many professional staff carry photos, PowerPoint presentations, etc., around on thumb drives and may unintentionally bring malware back to the office. Need to emphasize that, and also create some new protocols and scanning ability.

This is one of the better security training courses I have taken

Offer it once in a career. If I mess it up after that, fire me.

Seriously, 1) Write it in plain English, not lawyer-bureaucrat-speak. THIS IS NOT A TEST ON ACRONYMS. WHO CARES WHAT THE ACRONYMS ARE? JUST WRITE OUT THE WORDS! MOST OF THIS SEEMED LIKE A TEST ON IRRELEVANT ACRONYMS. CUT THE STUPID ACRONYMS AND JUST WRITE OUT THE WORDS FOR ALL ALL THE CRAZY TERMS IN THIS TRAINING!!! 2) Make it more relevant to people outside of Washington and people with lower grades. This sounded like it was created by people in DC talking to other people in DC. At least have it reviewed by field people to see if this speaks to them.

You can improve this training by not putting text on top of graphics. The background images make the text hard to read.

I know this class is required for all employees, but the lack of hands-on exercises that require you to put this training into practice make it very difficult to retain the material. It also makes it borderline torture to take. I would recommend some kind of simulation that provides real-world scenarios that the student is required to complete. A series of slides with someone reading to you is not an effective way to deliver training.

Thanks for listening. Like the way you broke down in smaller sections with less confusing test questions for this version.

For those of us unfamiliar with "portable" technology, have a link that shows a photo of each item and an explanation (short paragraph) of how used by an individual. Also, make each screen/slide individually printable.

Additional examples of how DOI employees are often fooled into sharing PII

There was some changes that I have notice. No immediate changes need to be made. You guys are already doing a good job updating.

Professional communicators should write the content with input from subject matter experts. This looks like it was written by experts, and therefore it included asides and technical terms that were unnecessary.

Fix the technical piece that "launches in a new window". If one clicks on the links for more information it launches a new window. There is much labor cost that is tied to taking training and to aggravate the workforce more that it needs to be is something to address. I continue to repeat these matters every single time on these surveys. Please have this fixed. Also, these comments should go to BLM management not just contractors who have a stake in systems needing fixing.

Continue to package FISSA, Privacy and Records Management together. It is logical and efficient. Use agency specific examples. Maintain the first quarter of the fiscal year availability of the annual training. Previous, second and third quarter availability, coupled with connectivity issues, often resulted in "down to the wire" completion of this mandatory training.

Decrease background graphics as it makes it harder to read the information. Use lighter colors or place graphics outside the range of text.

Please give more specific on the job examples of how these rules apply

Get rid of the useless information about the underlying legislation. It is irrelevant.

Improve by having an editor review it. For example, words were missing from the read sentences, grammar was incorrect (e.g., the word "data" is a plural noun and requires a plural verb when used as a subject), etc.

give more examples of how these items relate to actual incidents in DOI that caused us to have to take this training. change the names or whatever to protect the innocent but make it apply to what has happened in DOI in the last year.

Have more examples of "is this a record?" with yes/no/maybe answers, so that people can look at specific things (especially email) and decide if it should be kept as part of an official file. This is the main issue we have with so many things being electronic. Also, some specific examples of the weaknesses most often discovered (how do our government systems keep getting compromised) might be useful.

The examples used in the course made me stop and look for times when I could apply the course material to my own situation. So... use more examples to illustrate the topics.

Text was very difficult to read when graphics were put behind it. DO NOT put graphics behind the text.

There is a new threat I heard about last week where someone can photograph your keys if you leave them on your desk, and create working copies in a short amount of time. This could be a problem for government facilities as well as people's homes. This might be something to touch on in a future training.

Optional step by step practice for decreasing risk on the smart phone and eliminating them. It's one thing to be aware, but being able to take it to the next level is important. For example, I don't know how to turn on the tracker (to locate a phone if it's lost or stolen).

The only question I missed was one worded with a double-negative. I see no point in that. I knew the content; it was just how it was worded that caused me to miss the question.

It would be nice if we knew how many modules there were in the course. That way you know where you are in the total training and if you will be able to finish it or if you will need to come back to it.

Allow a full-screen version of the training

Maybe reduce the length some of the lead-in slides. Some could be edited/wordsmithed a bit without losing content. Many of the graphics I'd seen before and didn't seem to quite fit what was being covered at that point in the content?

Many of the background graphics were very distracting from the content of the training. The background graphics need to be removed or made lighter.

More fliers or notices about the practices discussed in the training so the topics are not so foreign every year.

Please continue to check performance on satellite connection for field locations. So far it still works and saves progress most of the time. (Compared to anything from DOI university).

Updated examples in the Records Management and Privacy areas to demonstrate how the material should be applied. I didn't notice any changes to the content or information from previous years.

If you feel you will be successful in applying this learning please provide a few tangible examples of how you will apply it.

I am already a careful computer user. The one new aspect -- a link to international security information -- will be applied during international assignments.

Increased emphasis and specific directions on protecting identity card and using storage devices like DVDs, etc. I am a volunteer in a library and often provide NPS public domain information to public on such devices as USB drives and DVDs. My IT staff person recently helped me develop safer ways to do this. This course did not even mention them--only what we shouldn't do. All aspects of transferring NPS files and material to the public needs it's own treatment in a training program like this one.

I thought about using QR codes in some capacity but had not idea how vulnerable they are which will make me rethink my ideas.

I will remain cautious about opening emails from unknown sources, and even more cautious about opening those that look like they're from known sources.

I refer to this information each time I use by iPhone, every time I travel with my laptop computer, when reading and sending emails, and when using the internet to access information

I was surprised to learn Snowden had gotten people's passwords by them giving them to him because he said he needed it in the course of his work. We are all told not to give our passwords to anyone but we also do trust our IT folks so it's good to be reminded that the consequences of that can be dire.

I learned about the risk of downloading files from emails/risks of using wireless technology on mobile devices/to ask if my devices are encrypted/learned about phishing scams - will reduce my risk by changing how I use technology

I don't think I'm successful yet.

The content of this course is excellent -- particularly for individuals new to the agency/government and should be applied in all facets of our job.

i just started my position but so far the knowledge I have learned from the training has helped me in my position. Thank you!

I will apply what I have learned by thinking through my actions before taking any steps in regards to sensitive information.

I think it's good to be reminded of the importance of all the material presented. Although I cannot cite a specific use, the knowledge is: running in the background."

A year ago I was working with Microsoft support to fix a problem AT HOME. I got a call from a person who identified himself as from Microsoft support. I said to myself "Microsoft support calling me!???" yeah right, when does Microsoft support call anybody? So I said, "dude, who are you cause you're sure NOT from Microsoft." He tried and tried to get me to install a program that would give him control over my HOME computer. It was a fun game and I reported it to Law Enforcement. I could see how that would have been an easy trap for someone to fall into. The background sounded like a call center. I was happy to see that included in the training this year.

I will try to remember not to open ANYTHING I am not comfortable with, doesn't tie directly to my job, or that is a "chain letter" type correspondence.

Locking away sensitive information such as accountable forms and credit card information is absolutely crucial in my job, both from an ethical and exemplary employee standpoint. I treat this information as if it was my own so I am confident and comfortable that I am doing an above average job and securing sensitive information.

Will be careful about computer security and protecting personal information, and made some changes to our records management regime.

I am more cautious of leaving my workstation unattended, and now its a must to lock my computer. I am also looking at other ways to secure sensitive information and I am going to get better organize and label my information.

I will avoid viruses

Information stored in a cloud will now be backed up.

I will be a lot more vigilant in protecting the information in my office.

Identifying improper email that is being sent to my work computer. Also being able to utilize this practice with my home email. Properly storing employee PII Information and documents. As they are already being properly secured and maintained, just continuing with that same process.

My passwords have become stronger each time I've taken the course.

I'm more conscious of potential phishing attempts in my inbox. I've caught a few, and avoided opening malicious links or documents, as a result of what I've learned in FISSA training.

I will always be aware that I am the weak link. If I am not vigilant to who is over my shoulder or who has access to my office and I were to leave the computer unattended it could mean bad things for FWS.

I am still doing research on this subject to protect myself more.

Because protecting the PII of individuals and my employer is important I appreciate being reminded to all the angles bad people try to hurt both. For me a lot doesn't apply but to have the heads up is fine.

I feel that I can now successfully accomplish my tasks by being extra careful with confidential information and my own personal information.

I will carefully check email that I receive from unknown source and I will delete them without opening them if they are not from a verifiable known source or a verifiable Federal source.

It's common sense IT security and security of other people's stuff. Really simple, and I don't need a class on it

I will stay out of prison.

It relates to private as well as public work being careful with sensitivity of information.

I have already changed some of my email and security settings on my iphone and personal computer.

I understand now what sensitive data is and the need to destroy it within the context of my position.

If just one is helped through the example I set, that's a beginning. If several are helped during my career, that's progress. If there is never an incident caused, because of practicing the training learned, by any of those we come in contact with, which have learned through both the example and training. That's success

I will be successful because I have awareness of information exchange threats. I therefore will be less likely to let any inappropriate information fall into the wrong hands or be the one who increases the risk of threats gaining access to or installing harmful problems into my employer's networks, systems and valuable data holdings.

-Always good to go over the security points as this ensures better adherence to these needs. - Email and other records in the records retention portion was well-covered and gives me more confidence in what to save as gov't records, or what can be discarded - Will work towards making sure these records are backed up better

I consistently teach Action-Oriented Definitions that together help to recognize persons, organizations, and digital systems that are involved with corruption/abuse. The system of definitions allows an employee to connect what they are feeling to potential abuse in action oriented terms. "Practiced Expression" of the definitions triggers recognition of risk related to corruption and abuse. Unless people have an action-oriented definition to work with that relates to their emotions, they cannot logically connect subconscious perceived risks to actionable outcomes. Personal Health, Ethos (emotions and other subconscious agents), Pathos (social interactions), Logos (logical awareness with an emphasis on sustainability) defines the human experience. CORRUPTION = UNETHICAL AND/OR ILLEGAL ALLOCATION OF RESOURCES AND/OR OPPORTUNITIES RACKETEERING = ANY COALITION OF TWO OR MORE PERSONS AND/OR CORPORATIONS ACTING WITH INTENTION TO PROMOTE CORRUPTION TREASON = ANY SOCIAL GROUP REPRESENTATIVE WITH INTENTION TO WEAKEN SOCIAL GROUP SECURITY FOR THE PURPOSE OF PROMOTING CORRUPTION Treason can be with respect to localized organizations, or nationally. In a perfect ethical society, treason at any level indirectly is treason at the national level. However, because of the complexity of individual health, logical, emotional, and social systems throughout society, treason within an organization does not mean that treason at the national level is necessarily implicated. Common Sense = Self-Esteem (the sharing of useful information and/or skills with peer groups) + critical thinking + predicting consequences with an emphasis on sustaining support of desired outcomes Respect = the communication process of sharing useful information and/or

skills with a peer group and the associated trust conveyed from the group Disdain = the communication process of sharing non-useful and/or destructive information and/or skills with a peer group and the associated distrust conveyed from the group Self-Esteem (group dependent) = the accumulating collection of events involving Respect and Disdain a person generates in each social group; and through empathy the individual detecting the trust conveyed to them by the group Self-Confidence = is attributed to one's self as the accumulating collection of useful outcomes relative to teaching one's self useful information and skills; the trust one has in completing a related proposed task Self-Respect = is attributed by others as the accumulating collection of useful outcomes relative to teaching one's self useful information and skills; the trust one has in having the support of others to propose acting upon a related task <If you can translate this for me, I would greatly appreciate it!>

Security awareness in computing is very good - a must have information - for any users of any devices to reduce risk for the organization. The course overall is useful! This newer version is much more better than in past years.

I became more aware of security. Why are we taking these precautions and why does this training matter given that OPM can allow the Chinese to hack into all of our personal records and data?

The Information Systems Security Awareness was the most currently applicable part for my job. Each time I take this training it is a reminder and perhaps an update on how to guard against risk to digital info. and info. systems I use. It reminds me of the measures I should take to prevent putting my PII at risk in the course of my personal as well as professional life.

It is always a good reminder! I enjoy reviewing the material each year.

I have served in my current position for 14 years, and have taken this or similar training for most of those years. I have kept current with changing rules and laws, and this training always helps to refresh or update me on what is the latest requirements, threats and technology.

I remove my PIV card immediately after logging into my account and I lock my computer whenever I step away from it. I forward any suspicious phishing or scam emails to our IT staff. I am cognizant of the security risk of bringing (unsecured) personal memory devices into the office. I am very cautious around the handling of PII, though a very small portion of my work involves PII in any form. I change my password routinely and use a system that adds both letters and punctuation to my password creation process. Any words that I may incorporate are not found in the dictionary. I turn my computer off when I leave most nights except when I leave it on for weekly updates, so the software is always up to date and the system secure.

In the normal day to day operations we often get involved in a great many action items that distract us from what should be a standard operating procedure. This course is a great "brain tune up" to make sure we keep on task and operate our electronic information systems according to best practice. A good training & certainly time well spent.

It helps me to keep my data safe--absolutely critical. A pain to do every year, but necessary as a reminder/refresher

One the job, I travel with my laptop, daily a computer is used, and by just being aware of the new methods being deployed to either access information or contaminated a computer, is good to know. A reminder of what not to do while traveling or what to do prevents the old mentality of "I've always done it this way" from making one comfortable and complacent. Thus potentially causing an incident.

I am participating in the closure of a Genetic Tree Seed facility and this training helped refresh my knowledge regarding the disposition of many of our program data files, resource library material and other records to insure I was disposing of or archiving records appropriately, very timely training in that respect.

This is the annual FISSA. It is the same thing every year. There is nothing new to apply.

My awareness level has increased. I never leave my computer logged in if I am not at my desk. I pay much more attention before opening e-mails and attachments. At home I make sure that my virus software is up to date. Finally my awareness level for scams and safeguard PII has increased.

This training was purely to reduce the risk of mishandling information, in its many forms. I have not had a security incident, partially as a result of taking this training, and previous year trainings.