



Countering Emerging Threats with an Effective Awareness Program

Karen S. Urban, CISSP

Federal Information Systems Security Educators' Association (FISSEA)
27th Annual Conference | March 18, 2014



Evolving Technology



- Personnel expect greater mobility, connectivity, and networking capabilities
- As a result, networks today are a mixture of organizational issued and personally owned smart phones, tablets, laptops and desktop systems



The Threat Landscape

Today cyber attacks on private, public and government information systems are organized, disciplined, aggressive, sophisticated, and are becoming all too common



Personnel = Vulnerability



Whether intentional or not, organizational personnel continue to be a leading cause of data breaches and network intrusions

36%

Of breaches were caused by inadvertent misuse of data by employees*

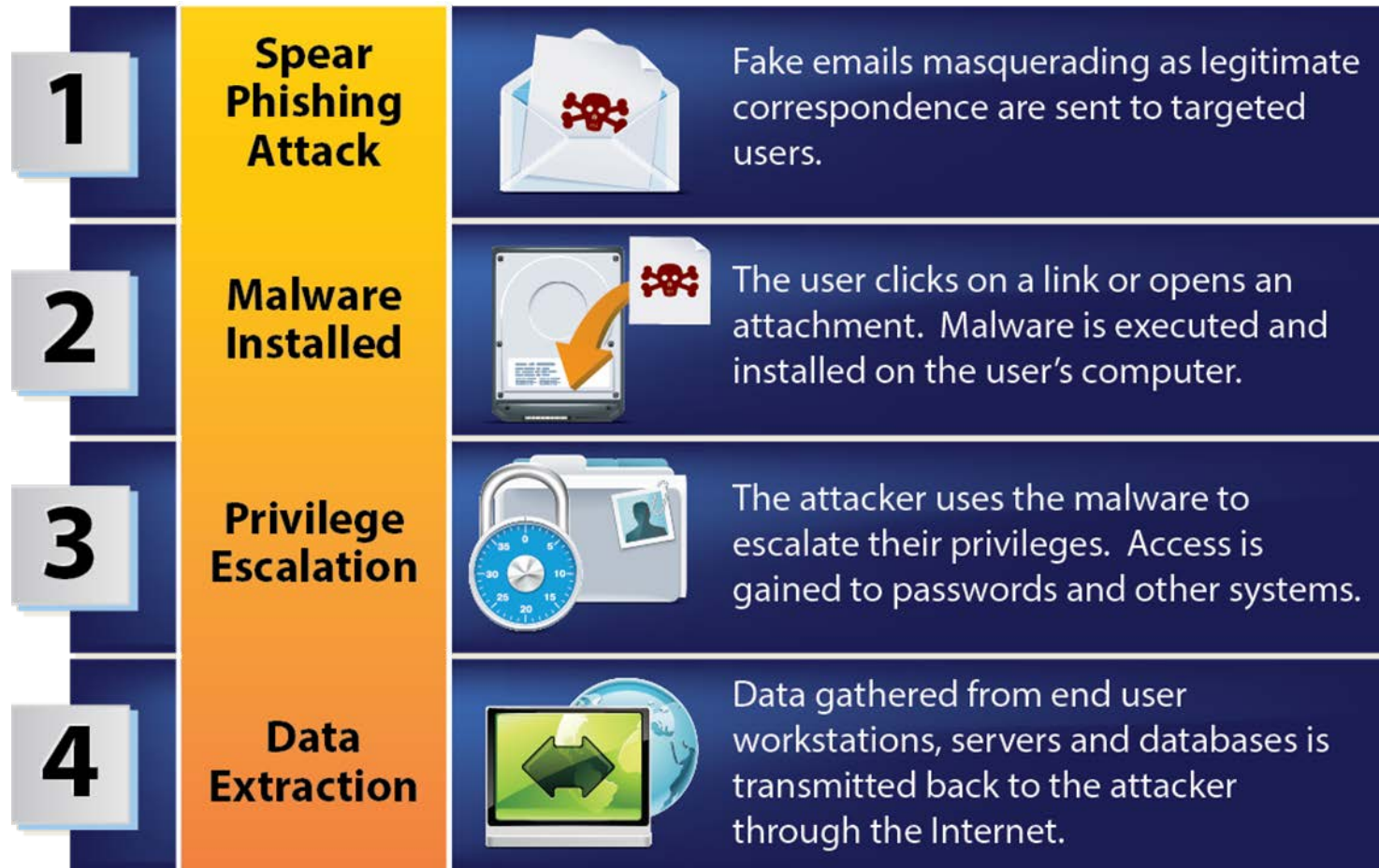


P@s5w0rd\$



76%
of network intrusions exploited weak or stolen credentials*

Willingness to “Click”



Good Intentions, Bad Results



Social Media Oversharing



How to Defend Against Ourselves

Implement, lead and sustain an active and aware cybersecurity culture!



Cyber Security Awareness Program

- Identify and target vulnerabilities introduced by human behavior
- Include real-life scenarios which people may actually encounter at work and at home
- Vary your delivery to capture and retain attention considering the range of learning styles that exist today
- Utilize metrics to measure effectiveness over time



Identify & Target Vulnerabilities Introduced by Human Behavior

- Analyze information contained in security incident reports, audit reports and Plans of Action & Milestones (POA&M)
- Examine organizational Policies and Procedures
- Consult with organizational Security and Privacy Subject Matter Experts (SMEs)
- Develop or Update a Security Awareness Baseline



Incident Reports



- Partner with members of your Security Operations Center and Incident Response Teams
- Analyze incident reports to identify incidents where the **root cause** was human behavior

Audit Reports and POA&Ms

- A closer look often reveals the root cause is human behavior
- Awareness training should be considered – even when a technical solution is recommended

Plan of Action and Milestones (POA&M)						
Measure		Instructions			Comments / Supporting Information	
FIPS 199 Risk Impact Level		Moderate				
FY 2014 System POA&M						
ID	Type of Weaknesses	Point of Contact (POC)	Scheduled Completion Date	Milestones (e.g. remediation actions) with Completion Dates	Source of Discovery	Status
1	Not all Access Control procedures listed in the SSP show evidence of having been updated within two years. MODERATE	John Doe	4/30/2014	Will document the review that was performed of the Access Control policies and procedures (Access Control SOP)	Security Assessment / Risk Assessment 09/25/2013, Finding #1	Completed: 3/30/2014

Issue 12. Data Transmission and Storage Restriction Can Be Bypassed
 By allowing users to use cloud storage and file sharing services (such as Google Drive), the Department enabled employees to bypass restrictions for transmitting data and storing agency information unencrypted using public cloud solutions. Department policy requires users to use e-mail systems when electronically sending and receiving government information, as well as encrypting all sensitive but unclassified data. OMB-06-16, "Protection of Sensitive Agency Information," states that when personally identifiable information is being stored at a remote site, NIST SP 800-53 should be implemented to ensure the information is stored only in encrypted form. However, Department policy does not provide any restrictions that regulate the

Issue 6. Data Storage on External Devices Process Needs Improvement (Repeat Finding)
 According to Department policy users are not allowed to save to external devices, such as flash drives or compact discs, without using Department-approved encryption, but there is no technical or automated solution to enforce this restriction. OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," states that agencies should encrypt, using only NIST certified cryptographic modules, all data on mobile computers and devices carrying agency data unless the data are determined to be not sensitive.

Policies and Procedures

- Identify potential gaps between requirements and actual implementation
- Review your Rules of Behavior (RoB)
- Consistent message between the awareness training program and other training

Rules of Behavior for Computer Network Users

As a computer network user, you must understand and agree to these rules of behavior prior to being granted access to the Department's computer network, which will provide you internet and intranet connectivity, electronic mail, network file storage, and network printing capabilities. You are accountable for your actions and responsible for the security of Department information. Upon being granted access to information resources, you will be held responsible for damage caused to Department information through either negligence or a willful act. Failure to follow these rules may result in legal action and/or disciplinary action up to and including termination of employment.



Consult with Security & Privacy SMEs



Gain insight to:

- Organizational strategies to mitigate risk
- New or updated policies and procedures



Develop or Update a Security Awareness Baseline

- Survey your personnel:
 - ✓ Identify areas where awareness is lacking or perceived challenges exist
 - ✓ Find out what they think will help them “behave in” instead of “behave out”
- Perform phishing exercises
- Informal outreach sessions



Learning Styles & Culture

- Telling is not learning
- E-reading (PowerPoint and e-learning as fancy PowerPoint) is not very effective except as an easy way to “check a box”
- Training only happens when the learner is “training” themselves, i.e., they must focus on the training to progress; they must engage with problem solving; and they must have repeated practice using gained knowledge and skills



Use Real-life Scenarios



- Training must be relevant to the learner
- Use real-life scenarios
- The more they can relate to and experience the scenario the more effectively they will remember what is being taught



Metrics & Continuous Monitoring

- Don't try to focus on everything; focus a few problem areas at a time!
- Deliver training more often (not only once a year) so you can address more topics throughout the year and based on real metrics

Use metrics like these to track progress and measure impact:

- # of personnel that successfully pass phishing exercises
- # of personnel that didn't pass phishing exercises
- # of personnel that report receipt of a phishing exercise email
- # of actual phishing incidents
- # of malware infected systems



Putting These Concepts to Work



Lyndon Baines Johnson: Conference Room

Your progress in this scenario:
2 of 4 answers correct.



[View this Scenario >>](#)

Cyber City Café

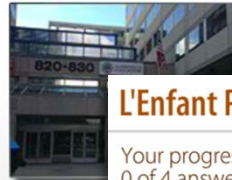
Your progress in this scenario:
0 of 4 answers correct.



[View this Scenario >>](#)

Union Center Plaza (UCP): Office

Your progress in this scenario:
0 of 4 answers correct.



[View this Scenario >>](#)

L'Enfant Plaza Metro

Your progress in this scenario:
0 of 4 answers correct.

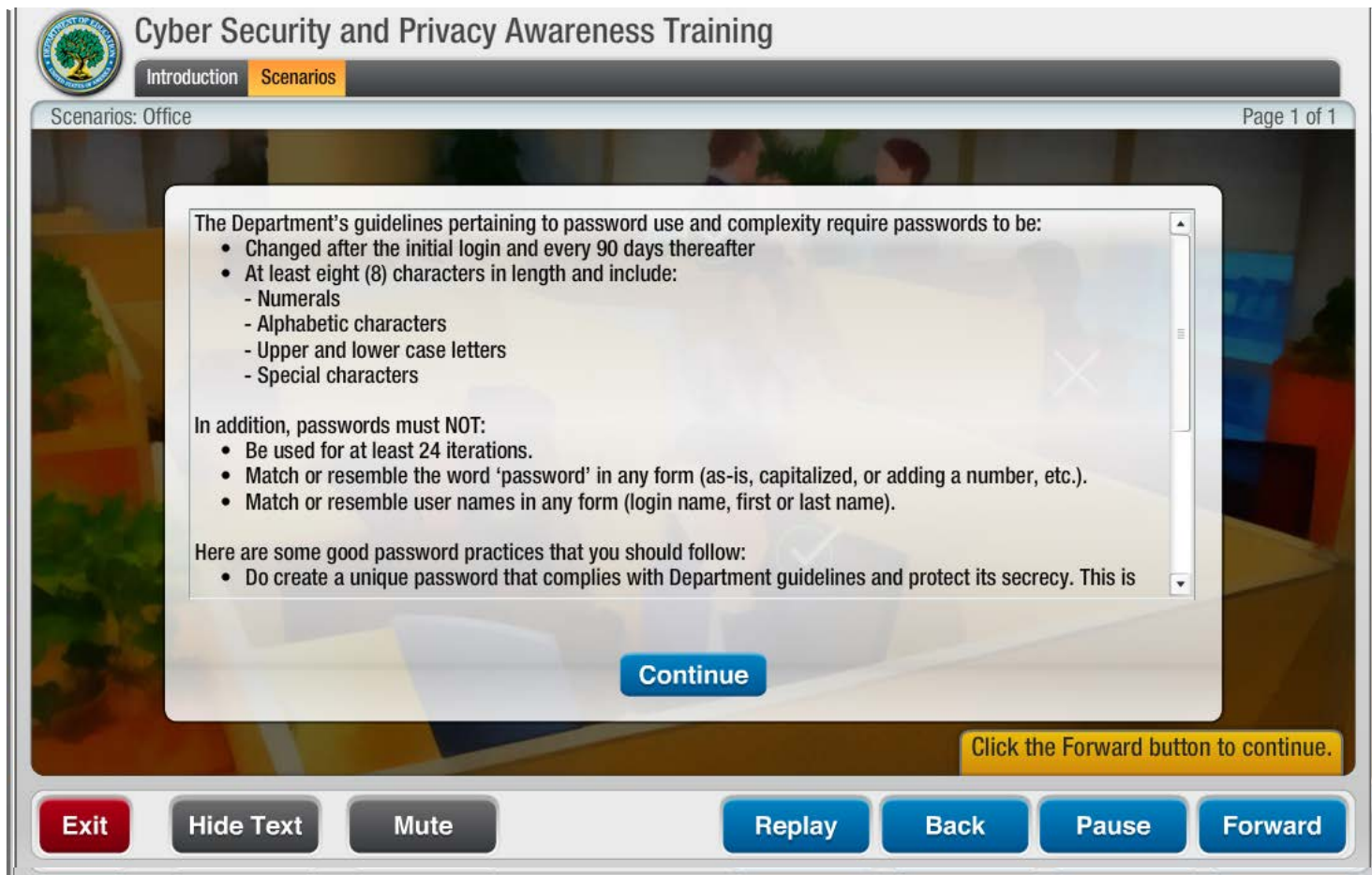


[View this Scenario >>](#)



The Department of Education's
FY 2014 Cyber Security &
Privacy Awareness Course

Real-life Scenarios in Action



The screenshot displays a training interface for the Department of Education. The main window is titled "Cyber Security and Privacy Awareness Training" and is currently on the "Scenarios" tab. The scenario is "Scenarios: Office". A dialog box is open, providing password guidelines. The dialog box contains the following text:

The Department's guidelines pertaining to password use and complexity require passwords to be:

- Changed after the initial login and every 90 days thereafter
- At least eight (8) characters in length and include:
 - Numerals
 - Alphabetic characters
 - Upper and lower case letters
 - Special characters

In addition, passwords must NOT:

- Be used for at least 24 iterations.
- Match or resemble the word 'password' in any form (as-is, capitalized, or adding a number, etc.).
- Match or resemble user names in any form (login name, first or last name).


Here are some good password practices that you should follow:

- Do create a unique password that complies with Department guidelines and protect its secrecy. This is

At the bottom of the dialog box is a blue "Continue" button. Below the dialog box, a yellow banner reads "Click the Forward button to continue." The bottom of the interface features a control bar with buttons for "Exit", "Hide Text", "Mute", "Replay", "Back", "Pause", and "Forward".



Repeat to Reinforce



The Aftermath of a Data Breach



Since mid-December 2013, many national retailers have experienced malware attacks targeted against their point-of-sale (POS) systems. These attacks resulted in data breaches which gave the attackers access to thousands of records containing payment card and personal information. One retailer reported the loss of payment card data for approximately 40 million customers and certain personal data for up to 70 million customers.

When we think of these breaches, a common assumption is that someone may acquire your credit or debit card details and use that information to drain your bank account or run up debt. However, with many payment card providers offering zero-liability protection, the highest risk to individuals whose personal data was compromised may come from spear phishing. Shortly after a breach occurs, attackers armed with knowledge of your email address, craft very convincing emails that appear to be from a retailer. Their goal is to trick you into revealing further personal information such as passwords or social security numbers that could be used to steal your identity. It is easy for attackers to obtain official looking logos and design an email so that it looks nearly identical to the routine communications you may regularly receive from a retailer such as monthly statements and weekly sales promotions. Be wary of any email message that asks you to verify your account, provide confidential information, click on a link, or open an attachment. Also, as information taken in a retailer breach may also include your phone number, stop and think before responding to phone calls to verify your account or recent transaction.

Here are a few things you should do:

- Don't enter sensitive information on a website at your own risk.
- Most of the time, if you see a suspicious email, don't click on the link or open the attachment.
- Legitimate emails should have a legitimate sender, a valid email address, and a phone number from the account.

Hidden in Plain Sight



Email messages are not always what they appear to be.

Some things deserve a second glance. Don't get tricked by a spear phishing attack.



MONTH OF 2013

guidelines pertaining to password size and complexity require passwords to be:

- Changed after the initial login and every 90 days thereafter
- At least eight (8) characters in length and include:
 - Numerals
 - Alphabetic characters
 - Upper and lower case letters
 - Special characters

In addition, passwords must NOT:

- Be used for at least 24 iterations
- Match or resemble the word "password" in any form (as-is, capitalized, or adding a number, etc.)
- Match or resemble user names in any form (login name, first or last name)

Here are some good password practices that you should follow:

- Don't use personal information such as birthdays or names of family members, friends, pets, sports teams, bands, etc.
- Don't use common phrases or words found in the dictionary, including foreign languages - hackers even have a Klingon dictionary!

Now that you understand how to create a strong password, commit it to memory and do not share your password with anyone, ever!

Incident Reporting

If you suspect a loss of Sensitive Personally Identifiable Information (SPI), or if you are aware of a privacy or security incident, you must notify your Information System Security Officer (ISSO) as soon as possible. If you are unable to reach your ISSO, please send an email to ISSO@ed.gov and privacy@ed.gov. Once the incident is reported, the Department's incident response team will determine if additional steps should be taken.

The FY14 Cyber Security & Privacy Awareness course is now available.

Training must be completed by July 31, 2014

Want Additional Information?

- Here are some links that you might find helpful:
- Avoiding Social Engineering and Phishing Attacks: <http://www.us-cert.gov/ncas/tops/5104-014>
 - Malware Targeting Point of Sale Systems: <http://www.us-cert.gov/ncas/alerts/13-002A>
 - Protect Your Identity from Security Breaches: <http://www.consumer.ftc.gov/topics/privacy-identity>
 - SplashData's Worst Passwords of 2013 Report: <http://splashdata.com/press/worstpasswords2013.htm>
 - Understanding Mobile Apps: <http://www.onguardonline.gov/articles/0018-understanding-mobile-apps>
- Contact Deborah.Coleman@ed.gov if you have additional questions.



Questions

For additional information, please contact:

Karen S. Urban

PMP, CISSP, CISA, CRISC, GPEN

Program Manager

M 979.220.6810 | O 979.260.0030

Larry D. Teverbaugh, Ph.D., PE

President & CEO

M 979.777.1127 | O 979.260.0030

<http://www.k2share.com> | Veteran Owned Small Business