



FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review rules before completing entry form including the due date. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Alexis Benjamin

Organization: Department of State, Office of Computer Security, Cyber Security Awareness Program

Type of Entry:

Awareness: there are four categories in this area: Poster, Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.), Website, Newsletter

Training & Education: there is one category for this area: Interactive scenario/exercise

Awareness Website

Title of Entry:

Description of Entry:

The Cyber Security Awareness Intranet site is a resource for DoS users, Information Systems Security Officers, program managers, and others responsible for implementing cyber security. The site contains various Cyber Security Awareness briefings, monthly campaigns, newsletters, Notes e-mails, points of contact, and a variety of awareness materials and resources.

Included is a screen shot of the main page as well as screen shots of two of our topic pages, Email and Phishing & Spear Phishing.

- View All Site Content
- Featured Topic
- Social Media
- Pictures
 - Posters
 - Web Banners
 - Signature Blocks
- Awareness Bulletins
- Awareness FAQs
- Cyber Guide Quarterly
- Cyber Security Notes
- AskCS FAQ
- Materials
- Videos
- Games
- Recycle Bin

DSNet > Diplomatic Security > Security Infrastructure Directorate (DS/SI) > Office of Computer Security > Cyber Security Awareness

CYBER SECURITY AWARENESS

The Cyber Security Awareness program encourages all Department personnel and contractors to be aware of their role in safeguarding information processed or stored on automated information systems used by the Department. This program, under the auspices of the Office of Computer Security, uses multiple mediums to convey its message.

Follow up on your
Cyber Threat
Brief

Google was at Main State.
Watch the video here.

Hot Topics



Email



Home Use



Identity Theft



Kids



Life Abroad



Malware



Mobile Devices



Online Shopping



Passwords



Phishing and Spear Phishing



Physical Security



Removable Media



Social Engineering



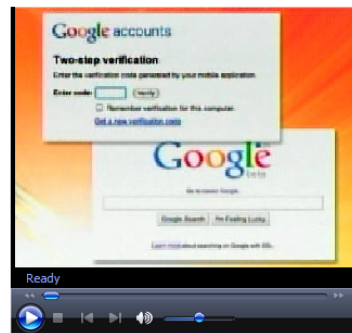
Social Media



Travel Tips



Web Surfing



Cyber Guide Quarterly

Read the third issue of our quarterly blog- *Cyber Guide Quarterly*.



Awareness Publications



Contact Us



Play Anti-Phishing Phil



PS800 Cyber Security Awareness Course



Take Our Survey

Email Security

Additional Resources

- 12 Tips for Better Email Etiquette
- How to Detect Spoofed Email
- How to Handle Suspicious E-mail
- Spam Checklist
- Phishing and Spear Phishing

Click here to learn more about Personal Email

Click image to open the PDF version.

Back to the list of Hot Topics

Cyber Checklist

E-mail

What is e-mail?

- Employees use e-mail to conduct official Department business
- Both your work and personal e-mail accounts are attractive targets for espionage or cyber crime

How can e-mail harm me?

- E-mail is one of the easiest and most widely used vehicles for hackers to:
 - Send spam, phishing, and spear phishing messages
 - Disseminate malicious links and attachments
 - Steal passwords or information
 - Spread malicious code and viruses

What do I do?

- Your work e-mail accounts are protected by special security measures that you do not have at home. Do not risk losing official data – avoid conducting official business on personal e-mail accounts
- Do not auto forward Department work to personal e-mail accounts
- Do not include personal e-mail addresses in out-of-office messages
- Always verify the sender and do not respond to requests for personal information
- Do not open suspicious attachments or click on suspicious links
- Use antivirus software to scan attachments before opening
- If you receive spam, e-mail spam@state.gov with the spam e-mail attached
- Learn about phishing and spear phishing, and where to send these messages

The Threat

Work-Related Spear Phishing

Phishing

On Your Personal E-mail?

Contact ISSO

Delete without opening

On Your Work E-mail?

Contact your ISSO, create a new e-mail, attach the e-mail in question, send to CIRT@state.gov

Contact your ISSO, create a new e-mail, attach the e-mail in question, send to CIRT@state.gov

Questions? Contact Awareness@state.gov

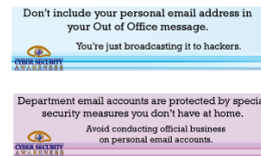
How to Handle Suspicious E-Mail			
Category	Example	Personal E-mail (Gmail, Yahoo, Hotmail)	State E-mail (OpenNet)
Spear Phishing	<ul style="list-style-type: none"> Unsolicited suspicious work-related e-mail Emails from fake government addresses 	Contact your ISSO	Contact your ISSO and create a new email, attach the email in question, send to CIRT@state.gov
Phishing	<ul style="list-style-type: none"> Unusual e-mail behavior from links UPS shipment notices 	Delete	Contact your ISSO and create a new email, attach the email in question, send to CIRT@state.gov
Spam	<ul style="list-style-type: none"> Viagra (prescription drugs) Nigerian scams 	Delete	Create a new email, attach the email in question, send to Spam@state.gov

If in doubt, contact your ISSO.

Posters (Click to Download)



Signature Blocks (Right Click to Download)



Web Banners (Right Click to Download)

Don't include your personal email address in your Out of Office message.

You're just broadcasting it to hackers.

Department email accounts are protected by special security measures you don't have at home.

Avoid conducting official business on personal email accounts.



Phishing and Spear Phishing

Additional Resources

- Spear Phishing Awareness Briefing
- Targeting of Personal Computers and e-mail
- Protecting Home Computers
- How to identify spoofed email
- Phishing Email Checklist
- Spear Phishing using S&ED Themes
- Massive Breach Compromises Customers
- Embassy Staff are Spear Phishing Targets

Click image to open the PDF version.

Back to the list of Hot Topics

Cyber Checklist
Spear Phishing

What is spear phishing?

- Is the e-mail targeted specifically to you for a reason?
- Does the e-mail contain specific info about you, e.g. work at the Department?
- Do you know the *real* sender? Is there a valid e-mail address?
- Is there a sense of urgency?
- Does the e-mail include fake or deceptive websites?
- Does the e-mail include misspellings and poor grammar?

How can spear phishing harm me?

- Someone could read or take over your Department or personal e-mail accounts
- Your compromised computer could give an intruder unauthorized access to Department computer networks and information
- Your compromised Department account could be used to further send spam, viruses, or malware to coworkers
- Your home or work computer could be infected with viruses that could make your computer unusable

What do I do?

- Do not click on suspicious links – type in the website yourself
- Do not open suspicious attachments
- Keep your home computer updated with the latest software security patches
- Do not conduct Department work on personal e-mail accounts
- Do not auto forward Department work to personal e-mail accounts
- Do not include personal e-mail address in out-of-office messages
- Learn about the risks also associated with phishing
- Learn to identify phishing by playing [Anti-Phishing Phil](#) online
- Send suspected, work-related spear phishing e-mails to the right authority

The Threat → **On Your Personal E-mail?** → **On Your Work E-mail?**

Work-Related Spear Phishing → Contact ISSO → Contact your ISSO, create a new e-mail, attach the e-mail in question, send to CSIRT@state.gov

Questions? Contact Awareness@state.gov

CYBER SECURITY AWARENESS

OnGuard Online

OnGuard Online provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.



Phishy Home



Phishy Office



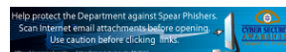
Phishy Store

Graphics

Poster (Click to Download)



Signature Blocks (Right Click to Download)



Web Banners (Right Click to Download)

