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.
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.

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.
Email Security

Additional Resources
- 10 Tip for Better Email Etiquette
- How to Detect Suspicious Email
- Spam Checklist
- Phishing and Spear Phishing

Click to open the PDF version.

Cyber Checklist

What is e-mail?
- Employers 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
  - 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 using 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 OpenState.gov with the spam e-mail attached
- Learn about phishing and spear phishing, and where to send those messages

How to Handle Suspicious E-Mail

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
<th>Personal E-mail (Email, Faxes, Reminders)</th>
<th>State E-mail (Outbox)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spear Phishing</td>
<td>Unsolicited suspicious work-related e-mail</td>
<td>Contact ISSO and create a new e-mail, attach the email in question, send to <a href="mailto:CITT@state.gov">CITT@state.gov</a></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>Unusual e-mail behavior from links</td>
<td>Delete</td>
<td>Contact ISSO and create a new e-mail, attach the email in question, send to <a href="mailto:CITT@state.gov">CITT@state.gov</a></td>
</tr>
<tr>
<td>Spam</td>
<td>Viral (prescription drugs)</td>
<td>Delete</td>
<td>Create a new e-mail, attach the email in question, send to <a href="mailto:Spam@state.gov">Spam@state.gov</a></td>
</tr>
</tbody>
</table>

If in doubt, contact your ISSO.

Posters (Click to Download)

Signature Blocks (Right Click to Download)

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

You're just broadcasting it to hackers.

Web Banners (Right Click to Download)

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

Avoid conducting official business on personal email accounts.
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.

Graphics

Poster (Click to Download)

Signature Blocks (Right Click to Download)

Web Banners (Right Click to Download)