fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

# *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:** **Shelly Tzoumas**

**Organization:** **US House of Representatives**

**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

**Website**

**Title of Entry:** **Microsite from House Information Security**

**Description of Entry:**

The INFOSEC Help desk is a microsite that compliments the formal publication of policy and procedure on the House Intranet. This microsite is message centered and contains behavioral cyber-safe tips and information for House staff. From here, staff can find helpful publications, animated explanation of current threats (like phishing and website drive by attacks). Included is helpful information for the office.

The Cyber Security Resources page offers download of all brochures and cyber safe brochures available from the Information Security Office.

Spyware, malware and zombies provides a brief explanation of common, and confusing, cyber terminology. Practical user tips are included on this page.

Anatomy of an Attack and How a Hacker Works are two instructional animations available here and used during in-office briefings.

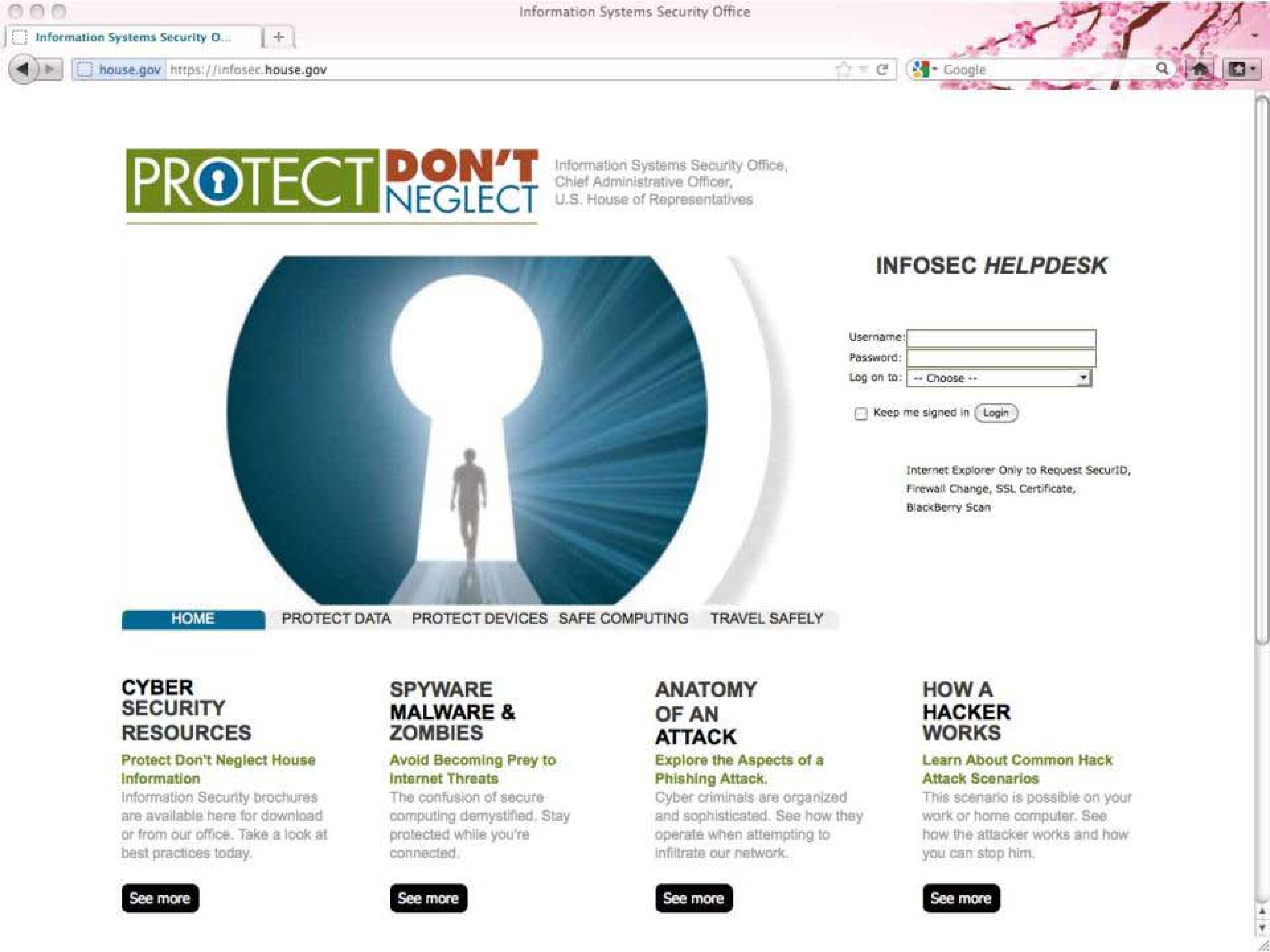
Protect Your Data offers instruction on how to consider the information and data an office produces and stores.  It reminds offices to know what data they have, consider what to keep and how to store sensitive data.

Protect Devices instructs offices on protecting the computers, printers, mobile phones and other network-aware devices.

Safe Computing offers users' common sense tips on computing in todays connected world.

Travel Safely concentrates tips and instruction on traveling and working remotely.

Each page offers links back into the House Intranet for policy and standards information.


Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov
Google

PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

## INFOSEC *HELPDESK*

Username:
Password:
Log on to: -- Choose --

□ Keep me signed in (Login)

Internet Explorer Only to Request SecurID, Firewall Change, SSL Certificate, BlackBerry Scan

HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY

### CYBER SECURITY RESOURCES

**Protect Don't Neglect House Information**

Information Security brochures are available here for download or from our office. Take a look at best practices today.

See more

### SPYWARE MALWARE & ZOMBIES

**Avoid Becoming Prey to Internet Threats**

The confusion of secure computing demystified. Stay protected while you're connected.

See more

### ANATOMY OF AN ATTACK

**Explore the Aspects of a Phishing Attack.**

Cyber criminals are organized and sophisticated. See how they operate when attempting to infiltrate our network.

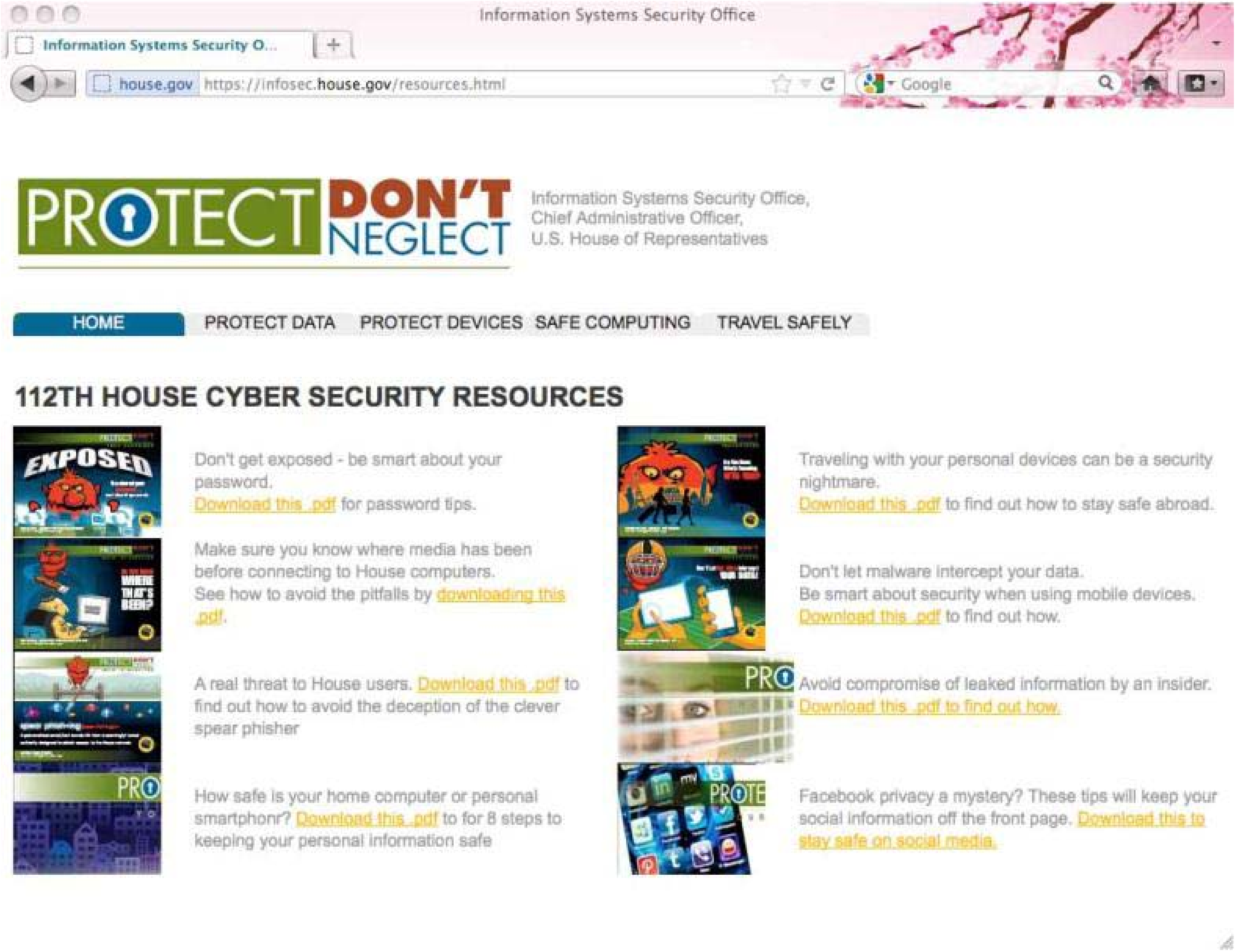
See more

### HOW A HACKER WORKS

**Learn About Common Hack Attack Scenarios**

This scenario is possible on your work or home computer. See how the attacker works and how you can stop him.

See more



Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov/resources.html
Google
PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

## 112TH HOUSE CYBER SECURITY RESOURCES

Don't get exposed - be smart about your password.
Download this .pdf for password tips.

Make sure you know where media has been before connecting to House computers.
See how to avoid the pitfalls by downloading this .pdf.

A real threat to House users. Download this .pdf to find out how to avoid the deception of the clever spear phisher

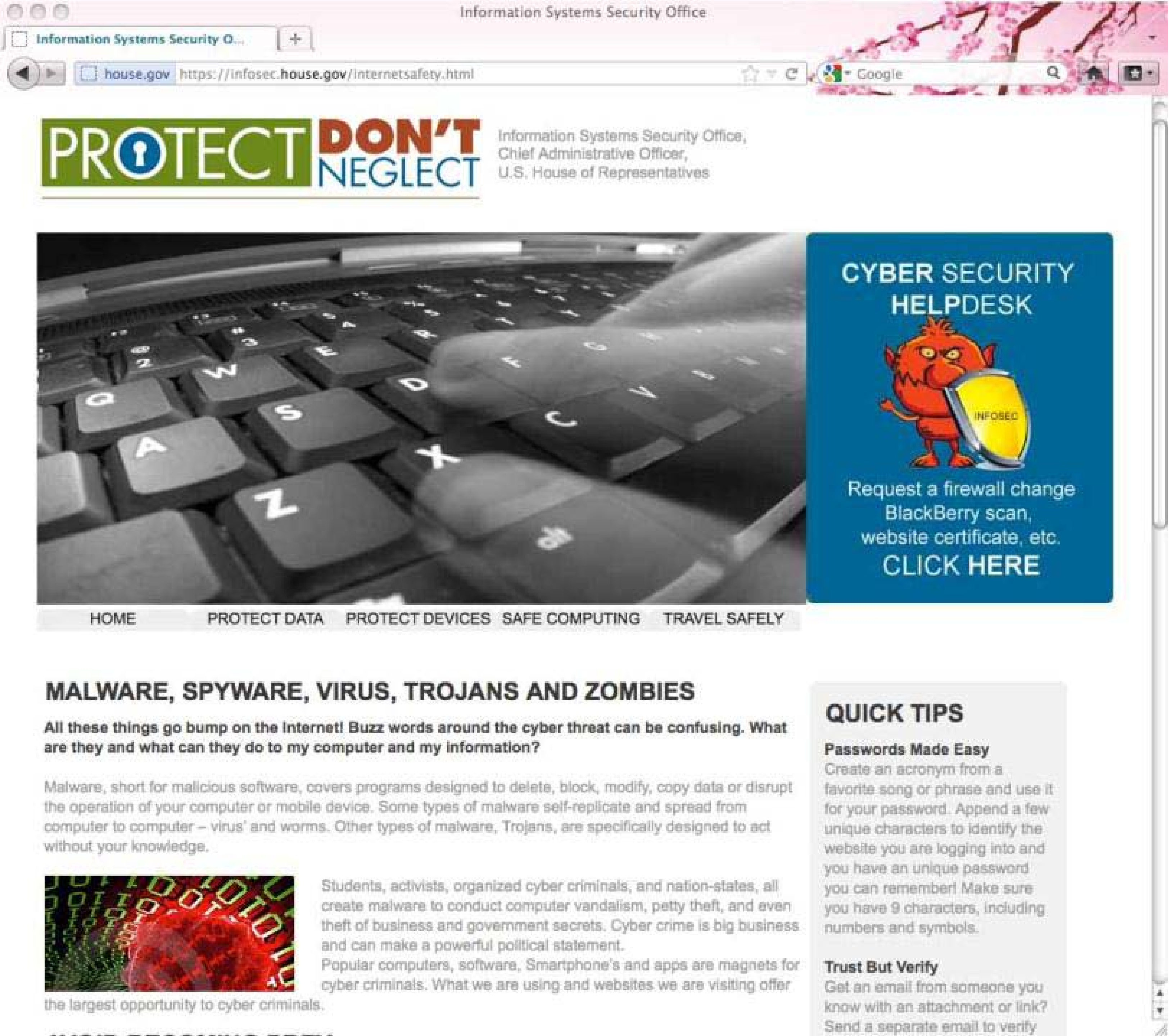
How safe is your home computer or personal smartphonr? Download this .pdf to for 8 steps to keeping your personal information safe

Traveling with your personal devices can be a security nightmare.
Download this .pdf to find out how to stay safe abroad.

Don't let malware intercept your data.
Be smart about security when using mobile devices.
Download this .pdf to find out how.

Avoid compromise of leaked information by an insider.
Download this .pdf to find out how.

Facebook privacy a mystery? These tips will keep your social information off the front page. Download this to stay safe on social media.


Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov/internetsafety.html
Google

PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

CYBER SECURITY HELPDESK

Request a firewall change
BlackBerry scan,
website certificate, etc.
CLICK HERE

HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY

## MALWARE, SPYWARE, VIRUS, TROJANS AND ZOMBIES

**All these things go bump on the Internet! Buzz words around the cyber threat can be confusing. What are they and what can they do to my computer and my information?**

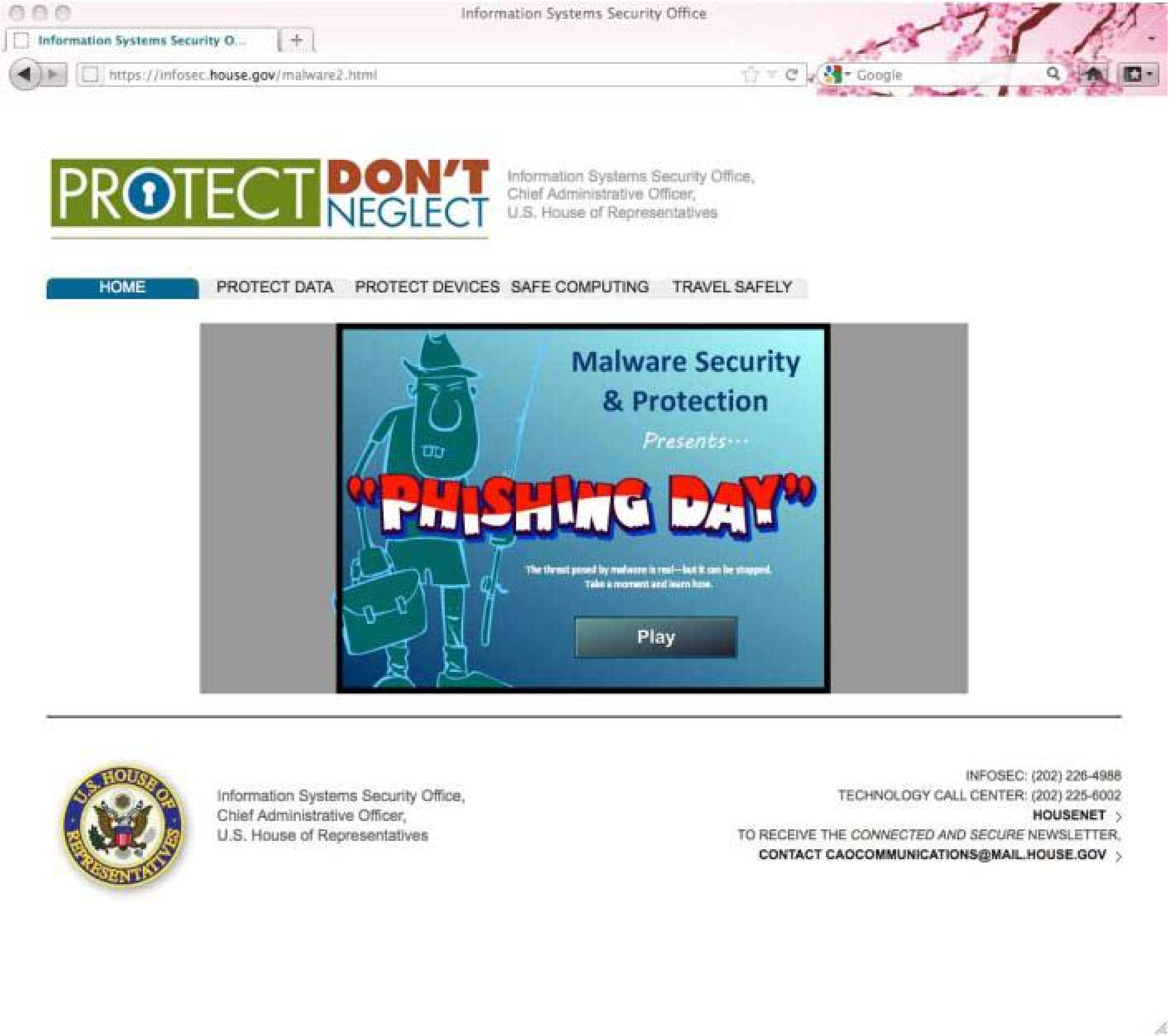
Malware, short for malicious software, covers programs designed to delete, block, modify, copy data or disrupt the operation of your computer or mobile device. Some types of malware self-replicate and spread from computer to computer – virus' and worms. Other types of malware, Trojans, are specifically designed to act without your knowledge.

Students, activists, organized cyber criminals, and nation-states, all create malware to conduct computer vandalism, petty theft, and even theft of business and government secrets. Cyber crime is big business and can make a powerful political statement.
Popular computers, software, Smartphone's and apps are magnets for cyber criminals. What we are using and websites we are visiting offer the largest opportunity to cyber criminals.

## QUICK TIPS

**Passwords Made Easy**
Create an acronym from a favorite song or phrase and use it for your password. Append a few unique characters to identify the website you are logging into and you have an unique password you can remember! Make sure you have 9 characters, including numbers and symbols.

**Trust But Verify**
Get an email from someone you know with an attachment or link? Send a separate email to verify


Information Systems Security Office
Information Systems Security O...
https://infosec.house.gov/malware2.html
Google
HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY
Play

PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

Malware Security & Protection

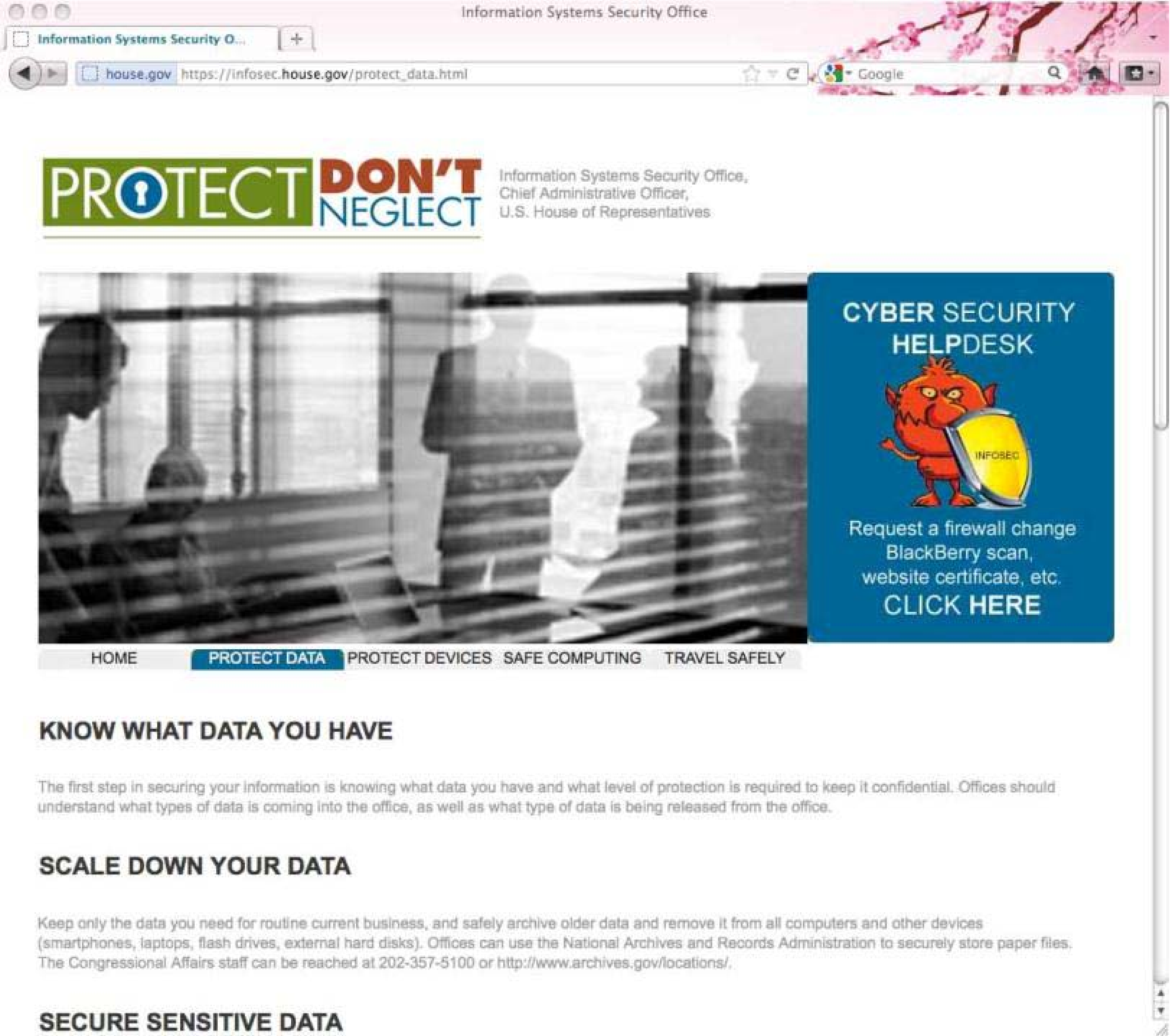
*Presents…*

"PHISHING DAY"

The threat posed by malware is real—but it can be stopped.
Take a moment and learn how.

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

INFOSEC: (202) 226-4988
TECHNOLOGY CALL CENTER: (202) 225-6002
**HOUSENET** ›
TO RECEIVE THE *CONNECTED AND SECURE* NEWSLETTER,
**CONTACT CAOCOMMUNICATIONS@MAIL.HOUSE.GOV** ›



Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov/protect_data.html
Google

PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

CYBER SECURITY HELPDESK
INFOSEC
Request a firewall change
BlackBerry scan,
website certificate, etc.
CLICK HERE

HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY

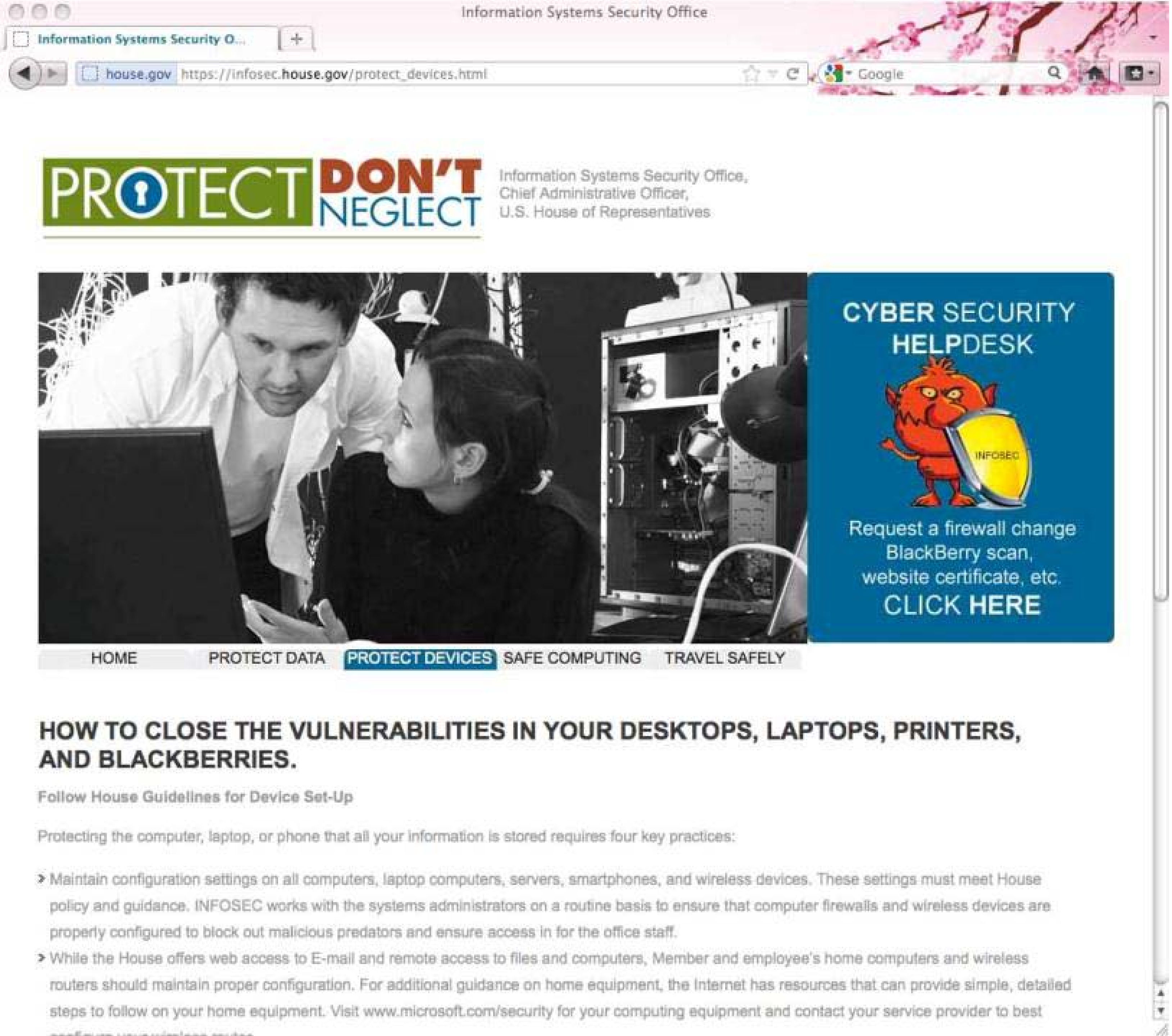
## KNOW WHAT DATA YOU HAVE

The first step in securing your information is knowing what data you have and what level of protection is required to keep it confidential. Offices should understand what types of data is coming into the office, as well as what type of data is being released from the office.

## SCALE DOWN YOUR DATA

Keep only the data you need for routine current business, and safely archive older data and remove it from all computers and other devices (smartphones, laptops, flash drives, external hard disks). Offices can use the National Archives and Records Administration to securely store paper files. The Congressional Affairs staff can be reached at 202-357-5100 or http://www.archives.gov/locations/.

## SECURE SENSITIVE DATA


Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov/protect_devices.html
Google

PROTECT DON'T NEGLECT

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

CYBER SECURITY HELPDESK

Request a firewall change
BlackBerry scan,
website certificate, etc.
CLICK HERE

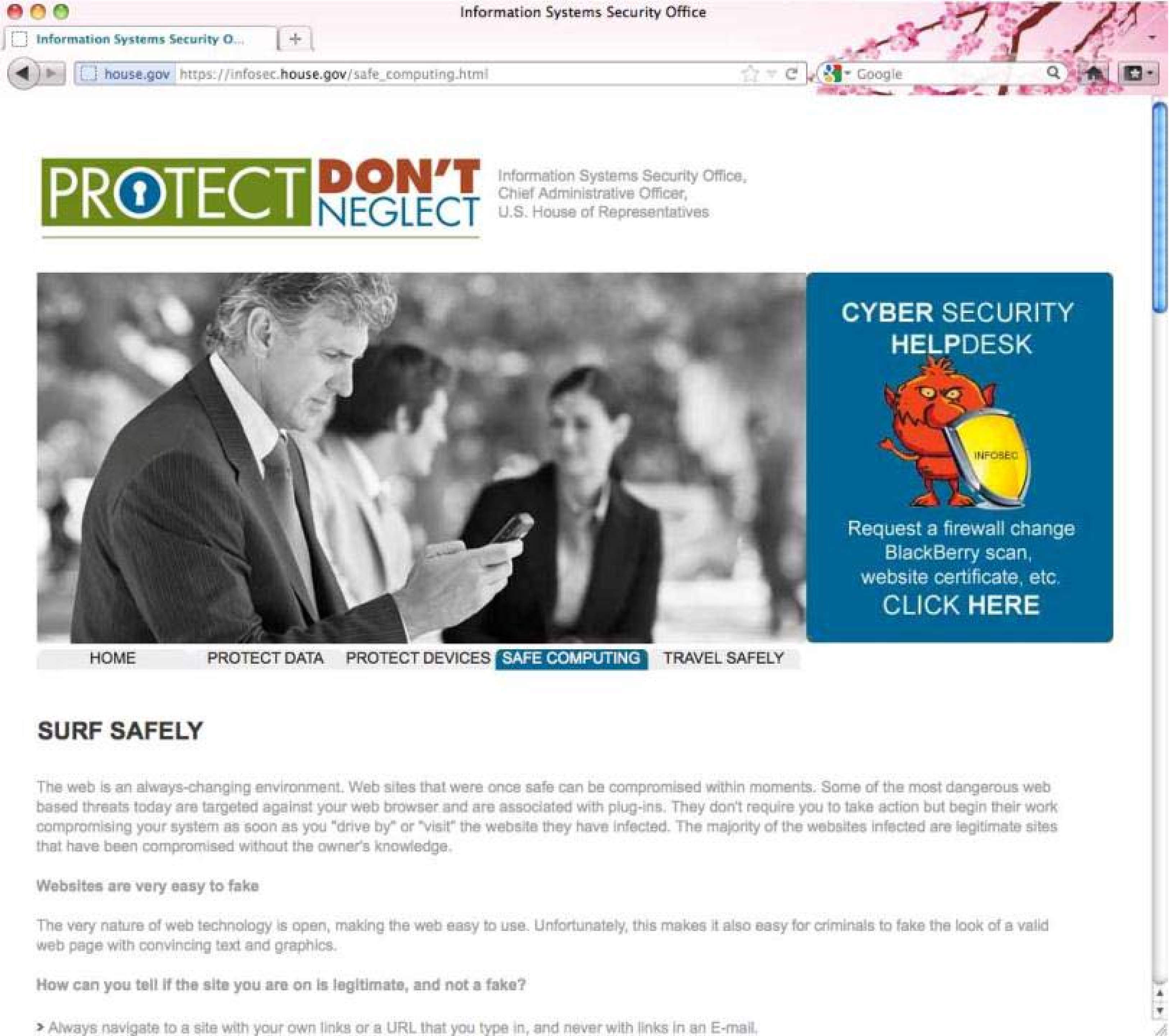
HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY

## HOW TO CLOSE THE VULNERABILITIES IN YOUR DESKTOPS, LAPTOPS, PRINTERS, AND BLACKBERRIES.

**Follow House Guidelines for Device Set-Up**

Protecting the computer, laptop, or phone that all your information is stored requires four key practices:

- Maintain configuration settings on all computers, laptop computers, servers, smartphones, and wireless devices. These settings must meet House policy and guidance. INFOSEC works with the systems administrators on a routine basis to ensure that computer firewalls and wireless devices are properly configured to block out malicious predators and ensure access in for the office staff.
- While the House offers web access to E-mail and remote access to files and computers, Member and employee's home computers and wireless routers should maintain proper configuration. For additional guidance on home equipment, the Internet has resources that can provide simple, detailed steps to follow on your home equipment. Visit www.microsoft.com/security for your computing equipment and contact your service provider to best configure your wireless router.



Information Systems Security Office
Information Systems Security O...
house.gov https://infosec.house.gov/safe_computing.html
Google
PROTECT DON'T NEGLECT
INFOSEC
HOME
PROTECT DATA
PROTECT DEVICES
SAFE COMPUTING
TRAVEL SAFELY

Information Systems Security Office,
Chief Administrative Officer,
U.S. House of Representatives

**CYBER** SECURITY **HELP**DESK

Request a firewall change
BlackBerry scan,
website certificate, etc.
CLICK **HERE**

## SURF SAFELY

The web is an always-changing environment. Web sites that were once safe can be compromised within moments. Some of the most dangerous web based threats today are targeted against your web browser and are associated with plug-ins. They don't require you to take action but begin their work compromising your system as soon as you "drive by" or "visit" the website they have infected. The majority of the websites infected are legitimate sites that have been compromised without the owner's knowledge.

**Websites are very easy to fake**

The very nature of web technology is open, making the web easy to use. Unfortunately, this makes it also easy for criminals to fake the look of a valid web page with convincing text and graphics.

**How can you tell if the site you are on is legitimate, and not a fake?**

> Always navigate to a site with your own links or a URL that you type in, and never with links in an E-mail.