

Center for Development of Security Excellence  
**CDSE**  
 Learn. Perform. Protect.



**Secure Communication**  
 (in an insecure world)

---

---

---

---

---

---

---

---

---

---

**The Internet Today** CDSE

Number of connected devices:  
**Over 10 Billion**

Internet users worldwide:  
 ~3 Billion  
 (40% of the world population)

eCommerce Industry:  
 \$1.5 Trillion Globally

Online data:  
 Unknown, but  
 Google stores ~ 15  
 Exabytes  
 (15,000,000  
 Terabytes) of  
 information

Approximate "weight"  
 of the Internet  
 (electrons in motion)  
 ~150g  
 (slightly more than a  
 baseball)

2

---

---

---

---

---

---

---

---

---

---

**Cybercrime** CDSE

19% of U.S. Organizations lost more than \$50k to cybercrime in 2013

7% lost more than \$1 Million

1.5 Million Cyber Attacks every year

\$781 Million in losses to cybercrime reported to FBI in 2013

47% of American Adults had their data stolen by hackers in 2014

47%

3

---

---

---

---

---



---

---

---

---

---

 **Poll** 

Which of the following do you use?

- Social media (Facebook, Twitter, etc?)
- Online banking
- Online purchases
- Cell phones
- Skype
- Online gaming
- Cloud Storage (including iCloud)

4

---

---

---

---

---

---

---

---

 **Social Media** 



“Websites and applications that allow users to create and share content, or participate in social networking.”

- Facebook
- Twitter
- Snapchat
- Reddit
- YouTube
- Pinterest
- Tumblr
- LinkedIn

5

---

---

---

---

---

---

---

---

 **Social Media Risks** 



- Malware** through links and infected ads
- Social Engineering** to get private information
- Hackers** obtaining sensitive information
- Foreign Intelligence** elicitation via social media
- Inadvertent Release** of information (OSINT)

6

---

---

---

---

---

---

---

---

 **Social Media Security** 

- Don't provide information that will allow others to answer your security questions
- Restrict what personal information you share, such as job title, location, interests, family details, etc.
- Remember that you don't control the site's security
- Remember OPSEC
- Securely configure your social network account (<http://www.cdse.edu/toolkits/cybersecurity/index.php>)

7

---

---

---

---

---

---

---

---

 **Online Banking Risks** 



- Hacking
- Secure login
- Phishing
- Usernames/Passwords
- "Fly by Night" banks

Dimitry Belorossoff, aka Rainerfox, was extradited from Spain in 2014

8

---

---

---

---

---

---

---

---

 **Online Banking Security** 



Be aware of phishing attempts



Type in the URL using https



Change and secure passwords regularly



Log out when done



Be wary of online banking in public



Install and update an antivirus and firewall

9

---

---

---


---

---


---


---

---



## Mobile Devices





Zhiyun Qian (UC Riverside) demonstrated up to a 92% success rate in hacking mobile devices in a lab environment

- 91% of Americans own a cell phone
- 63% of those use their phones to access the internet
- 21% only use mobile devices for internet
- 16 Million malware infections in 2014
- 25% of users have had phones lost/stolen

10

---

---

---

---

---

---

---


---

---


---

---


---



## Mobile Device Security



- Use "https" instead of "http" whenever possible
- Use a secure password
- Enable the "find my phone" features
- Beware of fraudulent Wi-Fi networks
- Be cautious when shopping online
- Be aware of scams/phishing
- Check privacy settings on apps
- Only install apps from trusted sources
- Delete unused apps
- Update apps/OS regularly
- Consider mobile security software



11

---

---

---

---

---

---

---

---

---

---

---

---



## Skype



### Microsoft Security Bulletin MS15-104

"Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege"

#### Public vulnerabilities in previous versions

Skype Vulnerabilities

The following list includes some of the most critical Skype vulnerabilities known to the security community. It was our hope that there is a working remedy in this list, please let us know and we will update it as soon as possible.

1. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
2. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
3. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
4. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
5. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
6. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
7. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
8. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
9. Skype (Skype for Mac, Skype Desktop, Skype for Linux)
10. Skype (Skype for Mac, Skype Desktop, Skype for Linux)



12

---

---

---

---

---

---

---


---

---


---

---

---

 **Online Gaming Risks** CDSE

- Social engineering
- Identity theft
- Account hijacking
- Malicious links
- Compromised servers/  
Insecure code
- Browsers risks and  
configuration



13

---

---

---


---

---


---

---

---

 **Online Gaming Security** CDSE

- Go with reputable developers  
and use their official launcher
- Use anti-malware and firewall  
software
- Use strong passwords
- Patch software/OS
- Update browser
- Be careful about links
- Remember OPSEC
- Beware of “admin mode”



14

---

---

---


---

---



---

---

---

 **Cloud Storage** CDSE

“A storage model where data is maintained, managed, and backed up remotely and made available via a network”



15

---

---

---

---

---

---

---

---

 **2014 iCloud Breach** **CDSE**



2014: 500 private images of celebrities obtained via automated brute force password guessing

- Russian security researchers discussed vulnerability
- Proof of Concept script released
- Script was modified and used to compromise accounts
- Images were initially traded and sold online for bitcoin
- Later shared freely via social media

16

---

---

---


---

---


---

---

---

 **Cloud Security** **CDSE**

- Two-factor authentication
- Strong passwords or pass phrases
- Use a secure host (physical and personnel security controls, contractual requirements, logs, legal and regulatory requirements, etc.)
- Use encryption when possible
- Know if you're using cloud backups



17

---

---

---


---

---

---

---

---

 **General Security Tips** **CDSE**

- Read up on common scams and threats
  - <http://www.ic3.gov/media/default.aspx>
  - <https://www.us-cert.gov>
  - <http://www.cdse.edu>
- Keep your systems and software patched and up to date
- For added security, consider encryption or a VPN
- Use strong and unique passwords for each account

18

---

---

---


---


---

---

---

---

 CDSE



19

---

---

---


---


---

---

---

---

 CDSE



**QUESTIONS / COMMENTS:**  
[CYBERSECURITY.TRAINING@DSS.MIL](mailto:CYBERSECURITY.TRAINING@DSS.MIL)

---

---

---

---

---

---

---

---