

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

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 (CVE-2015-1744, CVE-2015-1745) - Denial of Service Vulnerability
2. Skype (CVE-2015-1746) - Denial of Service Vulnerability
3. Skype (CVE-2015-1747) - Denial of Service Vulnerability
4. Skype (CVE-2015-1748) - Denial of Service Vulnerability
5. Skype (CVE-2015-1749) - Denial of Service Vulnerability
6. Skype (CVE-2015-1750) - Denial of Service Vulnerability
7. Skype (CVE-2015-1751) - Denial of Service Vulnerability
8. Skype (CVE-2015-1752) - Denial of Service Vulnerability
9. Skype (CVE-2015-1753) - Denial of Service Vulnerability
10. Skype (CVE-2015-1754) - Denial of Service Vulnerability
11. Skype (CVE-2015-1755) - Denial of Service Vulnerability
12. Skype (CVE-2015-1756) - Denial of Service Vulnerability
13. Skype (CVE-2015-1757) - Denial of Service Vulnerability
14. Skype (CVE-2015-1758) - Denial of Service Vulnerability
15. Skype (CVE-2015-1759) - Denial of Service Vulnerability
16. Skype (CVE-2015-1760) - Denial of Service Vulnerability
17. Skype (CVE-2015-1761) - Denial of Service Vulnerability
18. Skype (CVE-2015-1762) - Denial of Service Vulnerability
19. Skype (CVE-2015-1763) - Denial of Service Vulnerability
20. Skype (CVE-2015-1764) - Denial of Service Vulnerability
21. Skype (CVE-2015-1765) - Denial of Service Vulnerability
22. Skype (CVE-2015-1766) - Denial of Service Vulnerability
23. Skype (CVE-2015-1767) - Denial of Service Vulnerability
24. Skype (CVE-2015-1768) - Denial of Service Vulnerability
25. Skype (CVE-2015-1769) - Denial of Service Vulnerability
26. Skype (CVE-2015-1770) - Denial of Service Vulnerability
27. Skype (CVE-2015-1771) - Denial of Service Vulnerability
28. Skype (CVE-2015-1772) - Denial of Service Vulnerability
29. Skype (CVE-2015-1773) - Denial of Service Vulnerability
30. Skype (CVE-2015-1774) - Denial of Service Vulnerability
31. Skype (CVE-2015-1775) - Denial of Service Vulnerability
32. Skype (CVE-2015-1776) - Denial of Service Vulnerability
33. Skype (CVE-2015-1777) - Denial of Service Vulnerability
34. Skype (CVE-2015-1778) - Denial of Service Vulnerability
35. Skype (CVE-2015-1779) - Denial of Service Vulnerability
36. Skype (CVE-2015-1780) - Denial of Service Vulnerability
37. Skype (CVE-2015-1781) - Denial of Service Vulnerability
38. Skype (CVE-2015-1782) - Denial of Service Vulnerability
39. Skype (CVE-2015-1783) - Denial of Service Vulnerability
40. Skype (CVE-2015-1784) - Denial of Service Vulnerability
41. Skype (CVE-2015-1785) - Denial of Service Vulnerability
42. Skype (CVE-2015-1786) - Denial of Service Vulnerability
43. Skype (CVE-2015-1787) - Denial of Service Vulnerability
44. Skype (CVE-2015-1788) - Denial of Service Vulnerability
45. Skype (CVE-2015-1789) - Denial of Service Vulnerability
46. Skype (CVE-2015-1790) - Denial of Service Vulnerability
47. Skype (CVE-2015-1791) - Denial of Service Vulnerability
48. Skype (CVE-2015-1792) - Denial of Service Vulnerability
49. Skype (CVE-2015-1793) - Denial of Service Vulnerability
50. Skype (CVE-2015-1794) - Denial of Service Vulnerability
51. Skype (CVE-2015-1795) - Denial of Service Vulnerability
52. Skype (CVE-2015-1796) - Denial of Service Vulnerability
53. Skype (CVE-2015-1797) - Denial of Service Vulnerability
54. Skype (CVE-2015-1798) - Denial of Service Vulnerability
55. Skype (CVE-2015-1799) - Denial of Service Vulnerability
56. Skype (CVE-2015-1800) - Denial of Service Vulnerability
57. Skype (CVE-2015-1801) - Denial of Service Vulnerability
58. Skype (CVE-2015-1802) - Denial of Service Vulnerability
59. Skype (CVE-2015-1803) - Denial of Service Vulnerability
60. Skype (CVE-2015-1804) - Denial of Service Vulnerability
61. Skype (CVE-2015-1805) - Denial of Service Vulnerability
62. Skype (CVE-2015-1806) - Denial of Service Vulnerability
63. Skype (CVE-2015-1807) - Denial of Service Vulnerability
64. Skype (CVE-2015-1808) - Denial of Service Vulnerability
65. Skype (CVE-2015-1809) - Denial of Service Vulnerability
66. Skype (CVE-2015-1810) - Denial of Service Vulnerability
67. Skype (CVE-2015-1811) - Denial of Service Vulnerability
68. Skype (CVE-2015-1812) - Denial of Service Vulnerability
69. Skype (CVE-2015-1813) - Denial of Service Vulnerability
70. Skype (CVE-2015-1814) - Denial of Service Vulnerability
71. Skype (CVE-2015-1815) - Denial of Service Vulnerability
72. Skype (CVE-2015-1816) - Denial of Service Vulnerability
73. Skype (CVE-2015-1817) - Denial of Service Vulnerability
74. Skype (CVE-2015-1818) - Denial of Service Vulnerability
75. Skype (CVE-2015-1819) - Denial of Service Vulnerability
76. Skype (CVE-2015-1820) - Denial of Service Vulnerability
77. Skype (CVE-2015-1821) - Denial of Service Vulnerability
78. Skype (CVE-2015-1822) - Denial of Service Vulnerability
79. Skype (CVE-2015-1823) - Denial of Service Vulnerability
80. Skype (CVE-2015-1824) - Denial of Service Vulnerability
81. Skype (CVE-2015-1825) - Denial of Service Vulnerability
82. Skype (CVE-2015-1826) - Denial of Service Vulnerability
83. Skype (CVE-2015-1827) - Denial of Service Vulnerability
84. Skype (CVE-2015-1828) - Denial of Service Vulnerability
85. Skype (CVE-2015-1829) - Denial of Service Vulnerability
86. Skype (CVE-2015-1830) - Denial of Service Vulnerability
87. Skype (CVE-2015-1831) - Denial of Service Vulnerability
88. Skype (CVE-2015-1832) - Denial of Service Vulnerability
89. Skype (CVE-2015-1833) - Denial of Service Vulnerability
90. Skype (CVE-2015-1834) - Denial of Service Vulnerability
91. Skype (CVE-2015-1835) - Denial of Service Vulnerability
92. Skype (CVE-2015-1836) - Denial of Service Vulnerability
93. Skype (CVE-2015-1837) - Denial of Service Vulnerability
94. Skype (CVE-2015-1838) - Denial of Service Vulnerability
95. Skype (CVE-2015-1839) - Denial of Service Vulnerability
96. Skype (CVE-2015-1840) - Denial of Service Vulnerability
97. Skype (CVE-2015-1841) - Denial of Service Vulnerability
98. Skype (CVE-2015-1842) - Denial of Service Vulnerability
99. Skype (CVE-2015-1843) - Denial of Service Vulnerability
100. Skype (CVE-2015-1844) - Denial of Service Vulnerability

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
