DEPARTMENT OF THE NAVY

CYBER CRIME HANDBOOK

This handbook contains an overview of the definitions, criminal techniques, electronic laws, incident reporting and responses regarding cyber threats to Department of the Navy (DON) personnel and the global network infrastructure we rely on.

Contributors:

Naval Criminal Investigative Service (NCIS)
DON CIO Information Assurance & Critical Infrastructure Protection
DON CIO Privacy
Marine Corps Network Operations and Security Command (MCNOSC)
Navy Cyber Defense Operations Command (NCDOC)

GOLDEN RULES

- **Protect Yourself:** Protect your privacy and personal information online.
- **Use strong passwords:** Protect them and change them regularly (strong passwords include using the compilation of uppercase letters, lowercase letters, numbers, symbols, and the avoidance of dictionary words).
- **Stop and think of the ramifications before you click:** Before you provide information, open files or attachments, or download files from unknown senders, take a minute to stop and think before you click.
- **Back up important files.**
- **All government equipment should be used for authorized purposes only.**

BASIC CYBER CRIME DEFINITIONS

- **Hacking:** Computer or network intrusion providing unauthorized access.
- **Phishing:** A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information (see also page 21).
- **Vishing:** Similar to phishing but done specifically over Voice over IP (VoIP).
- **Internet Extortion:** Act or threat of hacking into and controlling various industry databases and promising to release control back to the company if funds are received or demands are satisfied.
- **Internet Fraud:** A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims and/or conduct fraudulent transactions with financial institutions or other parties.
- **Identity theft:** The wrongful acquisition and use of another person's identifying information in a way that involves fraud or deception, typically for economic gain.
- **Child Exploitation:** Using computers and networks to facilitate the criminal victimization of minors.

TECHNIQUES USED TO COMMIT CYBER CRIMES

- **Spamming:** Sending unsolicited commercial email advertisements for products, services, and Web sites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
- **Phishing:** A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, social security numbers, passwords, or other sensitive information. Internet scammers use email bait to "phish" for passwords and financial data from the sea of Internet users.
- **Spoofing:** Creating a fraudulent Web site to mimic an actual well-known Web site run by another party. Email spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different source. Spoofing hides the origin of an email message.
- **Pharming:** A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types in a legitimate Web address. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent Web site when the user types in a legitimate address.
- **Denial-of-Service Attack:** An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denials of service compromise the availability of the resource.
- **Distributed Denial-of-Service:** A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. This method often makes use of worms that can then attack the target to spread to multiple computers.

- **Virus:** A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.
- **Trojan Horse:** A computer program that conceals harmful code. It usually masquerades as a useful program that the user would want to execute.
- **Worm:** An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
- **Malware:** Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
- **Spyware:** Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
- **Botnet:** A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

LAWS

Regulations and laws

- **Computer Fraud and Abuse Act (18 U.S.C. §1030):** Specifies as a crime the knowing unauthorized access to the computers used by a financial institution, by a federal government entity, or for interstate commerce. Such crimes include knowingly accessing a computer without authorization; damaging a computer by introducing a worm, virus or other attack device; or using unauthorized access to a government, banking, or commerce computer to commit fraud. Violations also include trafficking in passwords for a government computer, a bank computer, or a computer used in interstate or foreign commerce, as well as accessing a computer to commit espionage.

- **Fraud and related activity in connection with identification documents, authentication features, and information (18 U.S.C. §1028):** Defines the knowing production, transfer, or possession of false identification and false documents as a crime. This statute also outlaws the possession of document-making implements such as computer files, hardware, or software.
- **Aggravated Identity Theft (18 U.S.C. § 1028A):** Adds an additional 2-year term of imprisonment in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during and in relation to any felony violation of certain enumerated federal offenses.
- **Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003 (18 U.S.C. §§1466A, 2251, 2252A, 2423):** Outlaws using computers to generate child pornography, or depicting minors in any obscene or sexual acts. The act enhances tools to protect children and more severely punish those who victimize children.

- **Fraud and related activity in connection with access devices (18 U.S.C. § 1029):** Outlaws the knowing production, use, or trafficking in counterfeit or unauthorized access devices such as any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service that can be used to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.
- **Wire Fraud (18 U.S.C. § 1343):** Prohibits wire fraud. Courts have recognized a variety of means of electronic communications as falling under the wire fraud statute, including facsimile, telex, modem, and Internet transmissions.
- **Certain activities relating to material involving the sexual exploitation of minors (18 U.S.C. § 2252):** Prohibits the transportation, distribution, receipt, and possession, by any means, including a computer, of material involving sexual exploitation of minors.
- **The Federal Trade Commission Act (15 U.S.C. § 45(a)(1)):** The consumer protection provisions of the act declare unfair or deceptive acts or practices in or affecting commerce unlawful.
- **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (15 U.S.C. § 7701) (18 U.S.C. § 1037):** Sets forth requirements and prohibitions, both criminal and civil, relating to commercial e-mail messages. Contains criminal prohibitions on sending sexually explicit e-mail that does not contain a label or marking designating it as sexually explicit. While DOJ enforces its criminal provisions, the FTC and other regulators enforce its civil provisions, notably requirements to transmit accurate e-mail header information and to provide a functioning opt-out mechanism. The FTC has also promulgated rules under CAN-SPAM, particularly with regard to additional restrictions on unwanted sexually explicit e-mails.

LAWS *(CONT)*

- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Pub. L. No. 107-56 (Oct. 26, 2001)):** Enhances investigatory tools including the authority to intercept electronic communications relating to computer fraud and abuse offenses. It authorizes the Director of the Secret Service to establish nationwide electronic crimes task forces to assist law enforcement, the private sector, and academia in detecting and suppressing computer-based crime, and allows enforcement action to be taken to protect financial payment systems while combating transnational financial crimes directed by terrorists or other criminals.
- **The Adam Walsh Child Protection and Safety Act (Pub. L. No.109-248 (July 27, 2006)):** Prohibits anyone from using innocent or misleading words or images, such as "Barbie" or "Furby," that confuse a minor into viewing a harmful Web site. The law also prohibits knowingly using the Internet to sell or distribute date rape drugs to an unauthorized purchaser or with the intent to commit criminal sexual conduct.

DON CIO VISION:
A Naval warfighting team armed with the secure, assured, accurate, and timely information to fight and win.

DON CIO MISSION:
Deliver secure, interoperable, and integrated IM and IT capabilities to the Marine and Sailor to support the full spectrum of warfighting and warfighting support missions.

SECNAVINST 5239.19, DON Computer Network Incident Response and Reporting Requirements:

1. Develop information security policies sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the DON.
2. Ensure coordination of Information Assurance (IA) and Computer Network Defense (CND) issues with other military departments, defense agencies, national level organizations, and DoD.
3. Report periodically, in coordination with other senior officials, to the Secretary of the Navy on the effectiveness of the DON IA and CND program, including progress on remedial actions.
4. Utilize the incident reporting information to assess the effectiveness of DON IA and CND policy and adjust as required.
5. Coordinate risk management across the DON by balancing threat against system/data criticality to identify and implement practical solution.
6. Ensure incident trends are captured and reflected in DON-wide policy.

1000 Navy Pentagon
Washington, DC 20350-1000
(703) 602-2975
www.doncio.navy.mil

MCNOSC Mission:
The MCNOSC provides global network operations and computer network defense of the Marine Corps Enterprise Network (MCEN) in order to facilitate seamless information exchange in support of Marine and Joint Forces operating worldwide. The MCNOSC concurrently provides technical leadership for service-wide initiatives that utilize the enterprise capabilities delivered by the MCEN.

Subsets of the MCNOSC are the Marine Corps Emergency Response Team (MARCERT) and the Vulnerability Management Team (VMT).

MARCERT Mission:
The mission of MARCERT is to enable global network operations of the MCEN through protection, detection, and effective response, in order to defend seamless information exchange to Marines and Joint operating forces. MARCERT functions include:

- Intrusion Detection/Prevention
- Incident Handling
- Forensics
- Auditing the MCEN for system mis-configurations

VMT Mission:
The mission of the VMT is to identify potential vulnerabilities and mis-configurations on Marine Corps networks and systems and subsequently correct them.

The objective of the VMT is to determine if vulnerabilities exist and provide the assessed organization with a comprehensive vulnerability report which lists the deficiencies and the corrective actions that should be taken.

MARINE CORPS - Incident Reporting

REPORTS INCIDENTS TO MARINE CORPS COMPUTER NETWORK DEFENSE SERVICE PROVIDER (CNDSP), THE MARINE CORPS NETWORK OPERATIONS AND SECURITY CENTER (MCNOSC)

NIPRNET	https://www.mcnosc.usmc.mil/
E-mail	commandcenter@mcnosc.usmc.mil
SIPRNET	http://www.mcnosc.usmc.smil.mil/
E-mail	commandcenter@mcnosc.usmc.smil.mil
Telephone	DSN: 278-5300 Commercial: (703) 784-5300
Facsimile	DSN: 378-1445 Commercial: (703) 432-1445
Plain Language Address	MCNOSC QUANTICO VA

NAVAL NETWORK WARFARE COMMAND

GLOBAL MISSION:
Naval Network Warfare Command (NNWC) creates warfighting and business options for the Fleet to fight and win in the information age. NNWC delivers and operates a reliable, secure, and battle-ready global network. They lead the development, integration, and execution of Information Operations for the Fleet.

NAVNETWARCOM PURPOSE:
To ensure our leaders have the information, mechanisms, and technology to make rapid and well-informed effects-based decisions, to degrade our enemies' decision capabilities, and to influence the decision-making of others in all phases of operations.

With the ever increasing threats posed by new technologies, NAVNETWARCOM supports Naval Criminal Investigative Service (NCIS) efforts to counter and mitigate cyber crimes on Navy networks.

Navy Network users who suspect cyber crime activities must immediately report their concerns to their Command Information Assurance Manager (IAM). The Command IAM will coordinate with, Command Legal representatives, Security Manager, Executive and Commanding Officer to execute appropriate actions in support of NCIS efforts to counter cyber crimes.

NAVY - Incident Reporting

REPORTS INCIDENTS TO NAVY CNDSP, THE NAVY CYBER DEFENSE OPERATIONS COMMAND (NCDOC)

NIPRNET	https://www.ncdoc.navy.mil/
E-mail	ncdoc@ncdoc.navy.mil
SIPRNET	http://www.ncdoc.navy.smil.mil/forms.php
E-mail	cndwo@ncdoc.navy.smil.mil
Telephone	DSN: (312) 537-4024 Commercial: (757) 417-4024 Toll Free: 1-888-NAVCDOC (1-888-628-2362) STU/STE: (312) 537-7952/(757) 417-7952
Plain Language Address	NCDOC NORFOLK VA

CYBER MISSION:
To provide integrated critical investigative, operational, and analytical products and services to protect the Department of the Navy's information infrastructure and support counterintelligence and criminal investigations in furtherance of the naval mission worldwide.

NCIS Cyber's responsibility is to help the Navy protect its information assets by:

- Integrating technology processes into criminal, fraud, and counterintelligence investigations and operations that defend DON information systems assets and infrastructure.
- Conducting national and local computer network intrusion investigations.
- Providing advanced forensic media analysis tools and techniques to support NCIS investigations and operations.
- Fusing computer network attack analyses with criminal and counterintelligence investigations and operations; producing intelligence products identifying adversarial tools, techniques, and methods of operation.
- Using advanced tools to identify indicators and warnings from proactive operations and intrusion investigations.
- Enhancing communication with counterpart agencies on matters involving national-level infrastructure attacks and coordinating/deconflicting investigations and operations with other Defense crimminal investigative organizations and the intelligence community.

NAVAL CRIMINAL INVESTIGATIVE SERVICE
(cont)

Governing Requirements

SECNAVINST 5430.107

"Mission and Functions of the Naval Criminal Investigative Service"

- NCIS has primary jurisdiction within the DON for certain cyber-related functions as they apply to DON computer networks (proactive operations and criminal investigations).

SECNAVINST 5239.3

"Department of the Navy Information Systems Security (INFOSEC) Program"

- NCIS shall maintain a staff skilled in the investigation of computer crime.

OPNAVINST 3430.26

"Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)"

- NCIS is responsible for investigating incidents of computer crime in support of C2 protection.

NCIS Role

- NCIS proactive measures focus on potential threats to identify and deter threats to Navy networks within the continental U.S. (CONUS) and outside the continental U.S. (OCONUS).
- Responsible for counter intelligence (CI) and counter terrorism (CT) cyber support to the Department.
- Conduct intrusion investigations both from the criminal and CI perspective.
- Coordinate with other law enforcement agencies to pursue those exploiting DON networks and obtain valuable, CI and CT intelligence from the cyber perspective.
- Produce Intelligence Information Reports on intrusions alerting the Navy, DoD and IC communities on exploits and methodologies.
- Conduct intrusion investigations to provide current and actionable intelligence identifying potential threats to the DON's information infrastructure.
- The NCIS Cyber Department plays a vital role in the protection of the Navy's intellectual property.
- The NCIS Cyber Department conducts investigations and operations on entities who attack the DON infrastructure via intrusions, malicious code, denial of service, and unauthorized access.
- Cyber investigations and infrastructure protection operations conducted by the NCIS Cyber Department are key components of the DON's strategic objective to integrate warriors, sensors, networks, command and control, platforms, and weapons into a fully netted combat force (Network Centric Warfare).

NCIS has a worldwide presence and should be contacted anytime it is believed Navy or Marine Corps information infrastructure has been attacked via intrusions, malicious code, denial of service, unauthorized access, or anytime criminal activity is suspected.

DON CYBER INCIDENT CATEGORY

Cat 1-9	Description
1	**Root Level Intrusion (Incident):** Unauthorized privileged access (administrative or root access) to a DoD system.
2	**User Level Intrusion (Incident):** Unauthorized non-privileged access (user-level permissions) to a DoD system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges.
3	**Unsuccessful Activity Attempted (Event):** Attempt to gain unauthorized access to the system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (i.e., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code.
4	**Denial of Service (DOS) (Incident):** Activity that impairs, impedes, or halts normal functionality of a system or network.
5	**Non-Compliance Activity (Event):** This category is used for activity that, due to DoD actions (either configuration or usage) makes DoD systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorized users.
6	**Reconnaissance (Event):** An activity (scan/probe) that seeks to identify a computer, an open port, an open service, or any combination for later exploit. This activity does not directly result in a compromise.
7	**Malicious Logic (Incident):** Installation of malicious software (e.g., trojan, backdoor, virus, or worm).
8	**Investigating (Event):** Events that are potentially malicious or anomalous activity deemed suspicious and warrants, or is undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
9	**Explained Anomaly (Event):** Events that are initially suspected as being malicious but after investigation are determined not to fit the criteria for any of the other categories (e.g., system malfunction or false positive).

How to recognize a spear-phishing attempt

The "from" field of an e-mail can be easily faked (spoofed). It might appear completely correct, or have a similar variation. For example: account_security@mypay.com

On the other hand, the message may come from a legitimate e-mail account, because that account has been compromised. For example: john.smith.yourboss@yourbase.mil

This can occur when the attackers obtain someone's login credentials and e-mail contacts in their address book in order to obtain more accounts.

How can I be sure?

Is the message digitally signed?

The importance of digitally signing your email messages can't be stressed enough.

Other recognition factors of phishing attempts:

1. Generic greeting
2. Fake sender's address
3. False sense of urgency
4. Deceptive Web links.
5. E-mail requires that you follow a link to sign up for a great deal, log in and verify your account status, or encourages you to view/read an attachment.
6. E-mails that appear to look like a Web site
7. Misspellings and bad grammar

Be cognizant of this threat. Before clicking on any Web link within a message or opening up an attachment, be sure the source of the e-mail is legitimate!

PHISHING/SPAM *(cont)*

User Reporting

NMCI users are encouraged to perform the following upon receipt of spam or unwanted e-mail:

1. Highlight the spam e-mail in your inbox but ***do not open it.***
2. Go to Edit, pull down the menu and select > Copy.
3. Paste the entire email into a new message and type the word SPAM is in the subject line.
4. Forward it to NMCI_SPAM@nmci-isf.com for Navy users or usmc_anti-spam@nmci.usmc.mil for Marine Corps users.

Prevention

Never give out any of the following information to unknown sources:

- Date / Place of Birth / Social Security Number
- Credit Card Number / Mother's Maiden Name
- Address / Phone Number

To do:

- Review credit reports at least once a year.
- Ensure secure online transactions by locating the closed lock icon at the bottom right side of your web browser before disclosing personal information.
- Unless absolutely necessary, do not store any financial information on a computer.
- Use strong passwords and do not allow programs to save passwords.
- Use virus protection software and firewalls to prevent the loss of personal information and/or the introduction of malware.
- Don't give out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact and know who you are dealing with.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

IDENTITY THEFT *(cont)*

Response

- Contact bank or credit card issuer to report fraud.
- Place a fraud alert with the following credit agencies:
    a. Equifax - 800-525-6285
    b. Experian - 888-397-3742
    c. TransUnion - 800-680-7289
- File an identity theft complaint with your local police department and the Federal Trade Commission:
    - Online: ftc.gov/idtheft
    - By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
    - By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

"Hackers, terrorists, or other nations could use information warfare techniques as part of a coordinated attack to seriously disrupt electric power distribution, air traffic control, or financial sectors."

> ** Statement for the Record by the Director of Central Intelligence to the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, "Foreign Information Warfare Programs and Capabilities" (June 25, 1996).*

"September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them."

> ** Statement of the Director of Central Intelligence to the U.S. Senate Select Committee on Intelligence, "Current and Projected National Security Threats to the United States" (Feb. 6, 2002).*

The misuse of government equipment through downloading and installing illicit software can have a detrimental effect on the entire enterprise network by creating unauthorized "backdoors."

Providing personally identifiable information through methods of phishing, vishing, or social engineering will put yourself and others at risk. Your legitimate credentials can be used for unwanted and illegal activity, from identity theft to accessing government accounts.

GLOSSARY OF TERMS

- **Antispam Software**: Antispam software automatically intercepts and filters email before it reaches your inbox.
- **Antispyware Software:** Antispyware software helps protect your computer from spyware and other potentially unwanted software by detecting and removing known spyware programs. It can be scheduled to scan your computer at times that are convenient for you.
- **Antivirus Software:** Antivirus programs help protect you from malicious programs, called viruses, that attach themselves to a program or file in order to spread from computer to computer.
- **CNDSP**: Computer Network Defense Service Provider (i.e., MCNOSC and NCDOC).
- **Cookies:** Computer code that is placed on a hard drive when Internet users go to Web sites and allows the sites to identify the computer if it returns to the site.
- **Firewall:** A firewall will help protect your computer from hackers who might try to delete information from your computer, make it crash, or even steal personal information, such as passwords or credit card numbers over the Internet. If you use the Internet from home, installing a firewall before connecting to the Internet is the most important first step you can take to protect your computer.
- **Hacker**: A person who uses the Internet to access computers and information without permission.
- **Junk Email Filters:** First line of defense against spam. Many Internet Service Providers and email programs provide email filters.

- **Phishing:** Spam or a pop-up message to lure personal and financial information from unsuspecting victims.
- **Social Engineering:** Social engineering involves multiple correspondences to potential victims in order to get them to divulge critical and confidential information through trickery. Correspondence includes, but is not limited to, the use of e-mails, telephone calls and personal contact.
- **Spam:** Unsolicited commercial email. There are two types of spam, legal and illegal. The subject line is considered legally deceptive if it has a tendency or capacity to deceive consumers.
- **Spammer:** Someone who sends mass amounts of unsolicited commercial email.
- **Spim:** Instant message spam is also known as spim.
- **Spyware:** Programs installed without your explicit consent. Spyware can remotely control your computer or collect your personal information and send it to a third party.
- **Virus:** Software that spreads from computer to computer and damages files or disrupts your system.
- **Vishing:** Vishing is the use of social engineering and Voice over IP (VoIP) to gain access to private personal and financial information of a person.
- **Worms:** Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections.

REFERENCES

SECNAVINST 5239.3A, Department of the Navy Information Assurance Policy

SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements

Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01, Defense-in-Depth: Information Assurance (IA) and CND, of 8 Mar 06.

GAO report - CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats

Federal Trade Commission, www.ftc.gov

National Institute of Standards and Technology Computer Security Division, Comuter Security Resource Center, www.csrc.nist.gov