

2025
2026

Cyber Security Awareness Program



Table of Contents

About this Program	3
What is Information Security?	4
Principles of Security	7
Data Classification	9
Types of Information	10
Pillars of Cyber Security	11
Machine Level Security	12
Facilities and Physical Security	13
Machine Safeguards	14
Passwords and Access	15
Protections Against Unauthorized Use	17
Appropriate Use and Protection of Accounts with Elevated Privileges	18
Data Level Security	20
Data Protection and Safeguards	21
Proper Storage of Sensitive Information	22
Sanitation and Disposal of Storage Media	23
Network Level Security	24
Network Protection	25
Internet Level Security	26
Understanding Threats	27
What Is A Threat?	28
Who or What Causes the Problem?	29
Cyber Risk	31
Attacks	33
Recognizing Common Attacks	34
Types of Tactics Used in an Attack	35
Identifying a Phishing Email	38
QR code Precautions	39
Responding to Attacks	40
Reporting Attacks	43
AI in Cyber Security	44
Working Remote Best Practices	56
Training	57



About this Program

Meets guidelines of Texas Government Code section 2054.5191

This self-administered Cyber Security Awareness Program ^[1] designed to develop knowledge about the risks of computer usage, networks, and electronic devices.



Program Components:

- Cyber Security Lesson Plan (this document)
- Supplemental document of slides used in the Lesson Plan
- Cyber Security Awareness Handout
- Phishing: Doing Your Part and Red Flags Handout
- NCCoE Telework Security Overview & Tip Guide Handout
- Test for program comprehension
- Record of successful completion



Learning Objectives

- Know the basics of information security
- Be aware of the threats to information security
- Know motivations of threat actors
- Communicate best practices for your organization

Left Side Section:

- Includes additional supplemental information related to the current topic

What is Information Security?



Cyber Security Awareness Training

www.dcsdq.com



**Why Are You
Required to Have
Cyber Security
Training?**



**Texas Government Code
Section 2054.5191**

www.dcsdq.com



Your company or institution might have a directory on its website. In this case, anyone has access to your organization's email addresses and titles. Cyber threats are not necessarily a reason to remove this information because it is a service to your community and allows your company or institution to serve the public. This stresses the need for the education of email users.



- Full Name (if not common)
- Social Security Number
- IP Address
- Vehicle Plate Number
- Drivers License Number

PII
Personally Identifiable
Information

- Credit Card Number ■
- Date of Birth ■
- Birthplace ■
- Generic Information ■
- Fingerprints, Handwriting, Face ■

www.dcsdq.com

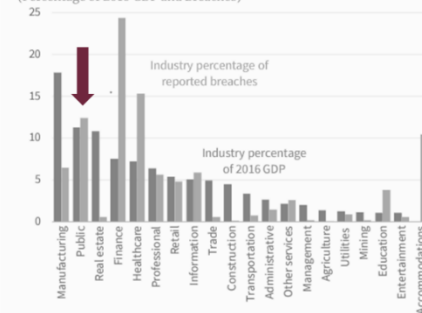
For example, when an institution is hacked by an outsider who wants information to sell, it is estimated that the response costs an average of **\$158 per record after the breach**. Examples of costs include detection, post breach response, notifying affected users, and lost business costs.



Cyber Landscape

[Public Sector: 13%]

Figure 6. Distribution of Security Breaches by Industry
(Percentage of 2016 GDP and Breaches)



Source: Bureau of Economic Analysis; Verizon; CEA Calculations.

www.dcsdq.com

The above slide indicates the impact of security breaches by industry, with the Public Sector noted by the red arrow. The Public Sector experienced 13% of breaches in 2016.



According to one study, cyber criminals got away with \$1.5 trillion in 2018 throughout the world. Many of these criminal activities start in other countries and it is difficult to stop.

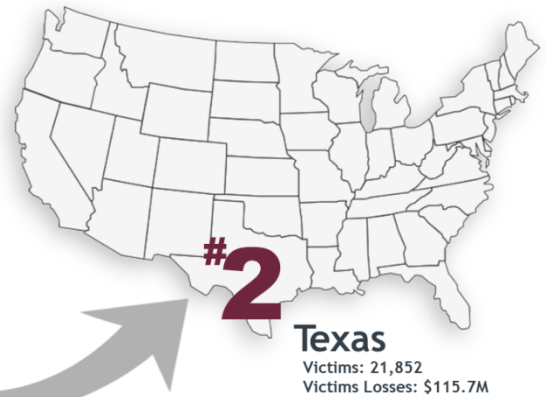
The City of Atlanta, Georgia was crippled by a cyber-attack in 2018 that affected many services and programs including courts, utilities, and parking.

We'll talk about ways to recognize scams and not be a victim.



Cyber Landscape

[Top 10 States by Number of Victims & Losses]



*According to FBI Internet Crime Report 2017

www.dcsHQ.com



Cyber Landscape

[Top 10 States Breakdown]

Victims		Losses	
CA:	41,974	CA:	\$214.2M
TX:	21,852	TX:	\$115.7M
FL:	21,837	FL:	\$110.6M
NY:	17,622	NY:	\$88.6M
PA:	11,348	AZ:	\$59.4M
VA:	9,436	WA:	\$43M
IL:	9,381	IL:	\$42.9M
OH:	8,157	NJ:	\$40.4M
CO:	7,909	CO:	\$39.9M
NJ:	7,657	MA:	\$39M

*According to FBI Internet Crime Report 2017


www.dcsHQ.com

Texas has a lot of people, so it's understandable that a large number of cybercrime victims are Texans. Texas is number 2 in the country in terms of the number of cybercrime victims and amount of losses.


Practicing safe computing and data storage will help not only our entity, but you personally. Think if criminals have your personal information and how they can exploit you with false credit cards.

Public organizations collect and store a lot of data that is of value to cybercriminals. The criminals illegally use stolen data such as credit cards, personal information, and health data. They also capture and hold data needed for daily operations in return for money through ransomware.

Principles of Security



Principles of Information Security



- Information Security
- Define the different types of information
- What information am I responsible for safeguarding

www.dcsdq.com

“Information security” is a broad term that covers protection of data and the systems that contain it, from the storage location through all connections to it. It includes the users who view, handle, and transmit it, and the devices they use to do so. The first step to developing a comprehensive information security plan and a culture of cyber-security is to recognize the need to have such a plan.

No user is safe from threats, no matter their position or authority. For an outsider who might want to intrude on or attack an organization, something simple like an org chart or address book can be valuable information. While it is obvious that certain information should be kept strictly confidential, something as mundane as the names and contact information of management or executives can be used against the organization in many ways.

Users should be cautious to the point of suspicion when dealing with any proprietary data. When entering a password or credit card number, sending an email or transferring a file, one should only do so on a known, managed system and connect through a known, managed connection.

Continual vigilance is a hard lesson to learn, but computers never rest, so users should understand that they should not falter in their procedures.



A high-level view lets us break down information security into smaller sections that would be managed by different groups. The IT department is not the only department that can make a difference in preventing cybercrime. The most important group is the organization's users. This means all of us are responsible for cybersecurity.

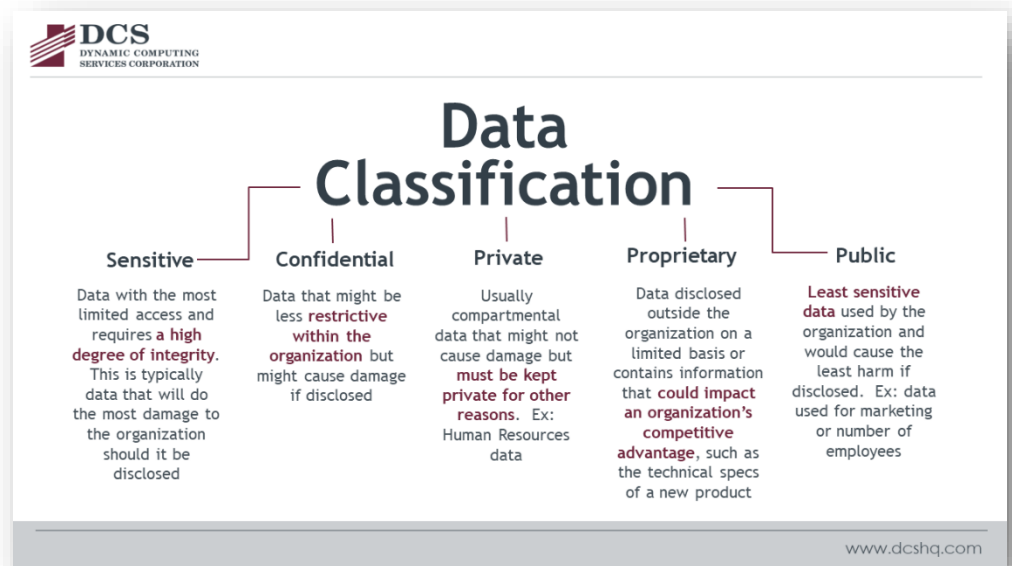
The cliché of a chain being as strong as its weakest link is applicable, for all the firewalls, anti-virus software, and encryption in the world is useless when a user clicks on something he or she should not click.



Procedures to classify data include:

- Set the criteria for classifying the data.
- Determine the security controls that will be associated with the classification.
- Identify the data owner(s) who will set the classification of the data.
- Document any exceptions that might be required for the security of this data.
- Determine how the custody of the data can be transferred.
- Create criteria for declassifying information.

Data Classification



The table above shows a way to classify data. This helps determine the security needed to protect it.

Additional Resource

<http://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=9>



Types of Information

You need to be aware of the forms of information and the location of the information that you are responsible for safeguarding.

Discrete files (MS Office documents, PDFs, image/video/sound, text) and folders containing said files.

Examples:

- Microsoft Word documents
- Microsoft Excel spreadsheets
- Microsoft PowerPoint files
- PDF
- Images
- Videos
- Any text document

Database files (for example files ending with .sql or .mdb or .accmdb).

Microsoft Access is a commonly used application that can be seen by users. In other applications, not many users will see the database file.



*See also: Cyber
Security
Awareness
Handout*

Pillars of Cyber Security



A cyber-security culture places the load on four main pillars:


Machine level - A user's computer(s) and other devices such as phones and tablets or personal computers should be treated with as much care as the data it contains

Data level - Treat the organization's data as if it was bundles of cash

Network level - No computer is an island these days, and things are connected in ways most users do not imagine even in the smallest office


Internet level - When connecting with the outside world, only let in exactly what you need, and only let out exactly what you are willing to give away.

Machine Level Security



4 Main Pillars of Cyber Security

[Machine Level Pillar]



The **Machine Level** includes work computers and devices, such as **phones** and **tablets**, or **home computers** that must be **treated with as much care as the data they contain**. The explosion in the use of personal computers and other personal electronic devices has led to innovation and production increases, but this ever-expanding use also creates potential risks.

www.dcsdq.com

The Machine Level includes work computers and devices, such as phones and tablets, or home computers that must be treated with as much care as the data they contain. The explosion in the use of personal computers and other personal electronic devices has led to innovation and production increases, but this ever-expanding use also creates potential risks.

Potential exposures to your organization:

- Weak passwords that are never changed allow hackers access to machines (single word passwords unacceptable)
- Anti-virus software is not installed or not updated
- Employees are not aware of dangers lurking related to cyber security
- Email rules and training are lacking or non-existent (clicking on links or attachments)
- Lack of control of flash drives and other portable connections
- No controls for accessing public Wi-Fi connections
- Lack of administrator controls to prevent downloading of apps or programs onto machines
- Lack of cyber security training



Facilities and Physical Security

Facilities have a role in safeguarding machines. You must guard against unauthorized access to facilities, data, and the systems on which it is stored.

Best Practices:

- Access to offices, data centers, warehouses, or any other workplace where computers are present should be strictly controlled. Once inside, further steps should be taken to guard information that is being accessed.
- Badged entry, with “tailgating” prohibited.
- Ensure outer doors are locked where possible, and those doors are not propped open (exits to smoking areas are notoriously porous due to frequent, repetitive use).
- Where possible, inner areas may require additional steps for entry. Non-employees should not be allowed to roam unattended.
- Monitors should be fitted with privacy screens to prevent over-the-shoulder theft of login credentials or sensitive data.
- Computers should be locked with passwords required to unlock whenever left unattended, including those for use in managing other devices like printers.
- Cabling and peripheral ports on all computers should be regularly inspected for sniffer devices, keyloggers, or other devices that could be monitoring computer input or network traffic.
- Networking devices (routers, switches, modems, networked computers such as servers) should be kept in locked areas.
- When possible, security guards should be employed to monitor building entry by non-employees.
- Locations such as rooms and control boxes that house electronic control systems, such as traffic lights, water and wastewater system controls, etc. should be securely locked to prevent tampering.



Note on machine level security—we often think about computers, tablets and smart phones as targets.

Consider other examples of machines at your institution— SCADA (supervisory control and data acquisition) systems for utilities, servers, traffic control boxes, streetlights, library computers, security systems, flood and tornado warning systems, and others.

Machine Safeguards

No computer should ever be left unsecure. It should be locked (electronically) while in use but locked up physically when not in use. Old computers can contain valuable data for a thief to exploit.

Obtain authoritative authentication to access the system.

For a mobile phone, prove you are who you say you are with Multi-Factor Authentication (MFA). Be aware that you should enable your mobile phone with passcodes, and fingerprint or facial awareness. It would be a big problem to lose your phone and an even bigger one to have it easy for a thief to access your texts, mail, social media, passwords, and payment apps.

Enable apps on phones and other portable devices to identify the device's location remotely. Common apps also allow you to lock, wipe, or disable the device remotely. These tools must be enabled BEFORE the devices get lost. Know your passwords and how to use the "find my phone" function.

Additional video resources:

Practical physical security:

<https://www.youtube.com/watch?v=b70-hr8RLzM>

Authentication:

<https://www.youtube.com/watch?v=t4kTgjQabV4>

MFA:

<https://www.youtube.com/watch?v=ZXFYT-BG2So>

Apple "Find my iPhone":

<https://www.youtube.com/watch?v=xt8W6K2IVVs>

Refer to your organization's procedures.



Multi-Factor Authentication (MFA) is Authentication using two or more different factors to achieve authentication.

Factors include:

(i) something you know (e.g., password/PIN);

(ii) something you have (e.g., cryptographic identification device, token); or

(iii) something you are (e.g., biometric)

Password management tools such as browser plugins, secure storage sites, or files stored locally with password records are common options but require study and decisions to be taken by each organization.

Passwords and Access

Passwords are a favorite topic in information security. There are many theories about how best to handle them, or even how to do without them. Until something better comes along, they must be managed and handled with care.

Best Practices:

- Password length is more important than complication. “P@\$\$w0rd!” is much easier for brute-force attacks to guess than “MyPasswordIsReallyLongAndThereforeSaferButStillNotReallySafe”.
- Avoid single words found in a dictionary or proper nouns.
- Do not keep a copy of passwords where others can see them, preferably not on paper anywhere, or in any clear-text electronic format.
- Do not share your passwords with anyone else.
- Do not use the same passwords, or close variation, on multiple systems, including personal ones.
- Enable Multi-Factor Authentication (MFA) on all systems possible. This system uses at least two ways to verify the person trying to access the system.

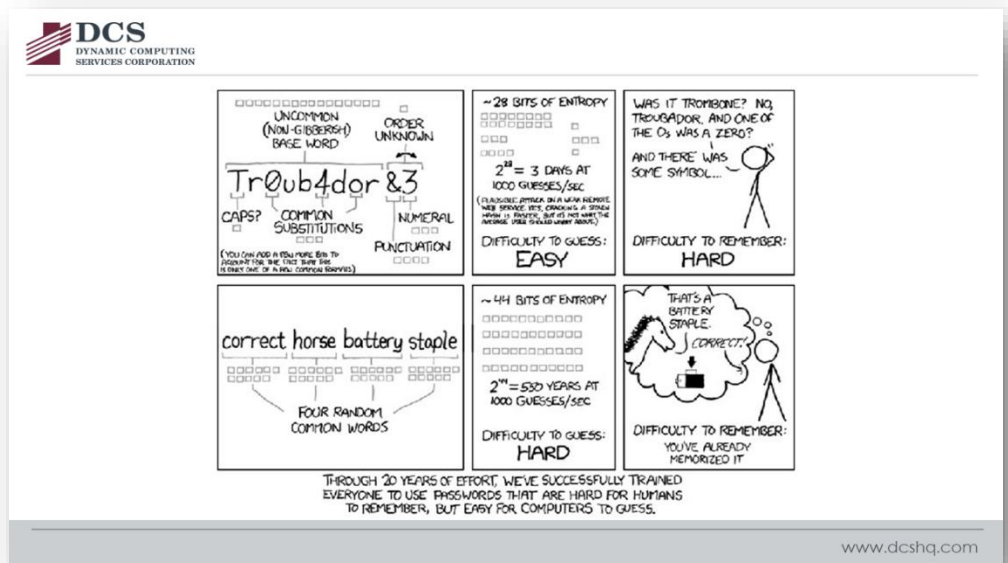
For example, some systems will send the user a text message with a code and the user must enter the code in addition to using their password on a computer.

Additional Resource:

<https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe>



Note: Cartoon XKCD
linked to
<https://xkcd.com/936/>
per the Creative
Commons License.



This slide shows the differences between two thoughts of selecting a password.

The top line says that a mixture of letters, punctuation, numbers, and symbols can be easy for computer programs to guess, while they are hard for the person to remember.

The second line of the comic strip points out that a longer password of random words is harder for a computer to guess but can be easy for the person to remember.

Systems sometimes have specific rules for passwords, so you might not have the choice, but consider this information if you do have a choice to have a long password, as it can be easier to remember.



Protections Against Unauthorized Use


Maintaining physical security is one part of effective defense. Keeping data secure is another. Several key elements to keep in mind are a combination of passive and active tools for retaining control of systems and the data they contain.

Best Practices:

- Password protection on every system, with Multi-Factor Authentication wherever possible.
- Always employ secure connections.
- Any system access credentials should be created by the IT department with proper roles, groups, and policies applied to the account before the credentials are given to a user.
- Credentials should not be shared, and passwords should be changed as quickly as possible if they ever are.

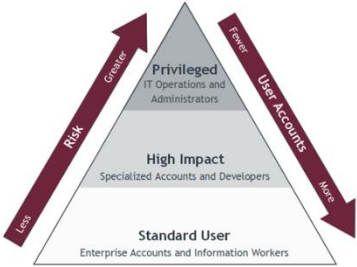


Appropriate Use and Protection of Accounts with Elevated Privileges



Protecting Accounts with Elevated Privileges

Privileged Account safeguards will include and extend Enterprise Account protections



High Impact Accounts

- Increased monitoring of usage with higher priority alerting
- Out-of-Band Tests

Privileged Accounts

- Role-Based Access Controls (RBAC)
- Just-In-Time (JIT) Entitlement
- Privileged Device Restriction
- Isolation between Control and Corporate accounts

www.dcsdq.com

Beyond the best practices and standard procedures in place for all Enterprise Accounts, additional protective measures should be taken for any higher risk account.

Organizations should have well-defined roles with established parameters for access and usage. Any elevated privileges should be granted and restricted around those roles.

High Impact Accounts

High impact accounts, such as Developer accounts, will typically require access to sensitive information such as databases, applications, and proprietary code.

Greater scrutiny must be given to data protection with these accounts, including:

- Increased monitoring of usage with higher priority alerting
- Out-of-Band tests for vulnerability and misuse

Privileged Accounts

Privileged accounts will be used by IT Operations and IT Administrators to access critical Control and Management systems.

Keeping these accounts secure is a top priority for any organization and should include:

- For passwords, an even more stringent password policy with greater complexity and shorter lifecycles.
- Use of key-based authentication and passwordless methods where possible.
- Implementation of Role-Based Access Controls (RBAC) - User accounts should be regularly audited, particularly when a User moves laterally, to ensure proper privilege levels are maintained or updated for new roles.
- For environments with centralized User Management, such as those utilizing Microsoft Active Directory or Entra, use of a Just-In-Time (JIT) Entitlement mechanism to provide elevated credentials only when needed. Credentials will be valid for the shortest time necessary and revoked when tasks are completed.
- Privileged Access Devices - Dedicated and locked-down devices or workstations used by authorized personnel to administer systems over a secure connection. Individual systems will also be configured to restrict connections and only allow for access from designated, privileged devices.
- Isolation between Control or Management accounts and Corporate accounts - Day-to-day activities should be conducted via standard Enterprise accounts, without additional privileges, on regular (non-privileged) devices.

Additional Resource:

<https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model>

Data Level Security



4 Main Pillars of Cyber Security

[Data Level Pillar]



The **Data Level** applies to the quantities, characters or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical or mechanical recording media. The **organization's data must be treated as it is "bundles of cash"** due to the efforts necessary to recreate, if even possible. In simpler terms, "once it's gone it's gone".

www.dcsHQ.com

The Data Level applies to the quantities, characters or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical or mechanical recording media. The organization's data must be treated as it is "bundles of cash" due to the efforts necessary to recreate, if even possible. Data is like cash in that if you lose cash or it gets stolen, you will likely not get your individual dollar bills back. Once data is gone, it's gone.

Potential exposures to your organization:

- Employees are not aware of the data created by all organizations and the importance of that data or the cost and effort necessary to restore damaged or lost data (if possible, to be restored)
- "Off-site" data backup is not provided, or backups are not performed regularly
- Employees do not believe their organization's data is relevant or "important enough" for a cyber attack
- Organization's data is not encrypted to protect from hackers



Data Protection and Safeguards

Technical aspects of data security are handled primarily by IT staff. But users should be aware of proper handling techniques. Many modern techniques require little or no technical savvy but are still effective.

Best Practices:

- Data should be backed up regularly.
- Ensure Anti-virus and anti-malware is installed on your machine and configured to receive updates automatically when released.
- Ensure all your devices are patched at minimum once a month and receive critical updates automatically when released.
- Make sure your computer always connects to secure WiFi locations (do NOT connect to free public WiFi).
- Encrypt your data on USB drives and other portable media.
- Ensure your computer, mobile devices, and tablets have auto-lock feature turned on and require a password to unlock.



Proper Storage of Sensitive Information

One puzzle to be solved in a cyber-secure culture is developing the ability to store data safely without the protective layers becoming a hindrance for authorized users.

Best Practices:

- Keep your workspace clean both in terms of securely destroying sensitive data on paper or hardware when not needed
- Keep their electronic spaces clean as well, deleting old or obsolete files and not leaving copies of sensitive material in different locations
- Follow guidance and rules for password length and complexity, and enforce periodic changes to passwords, ensuring one of the rules is dissimilarity to recent passwords.
- All network traffic should be conducted with secure connections between every point, including between servers, routers/switches, and the user's device.
- Users should never connect to a network or enter their credentials into a system they do not control, or connect to a public Wifi, especially one that does not require a password.
- Storage media (USB/flash drives, CD/DVDs, floppy discs, zip discs, tapes) should be kept in secure areas and handled as if it was cash.
- Contractors or vendors should be vetted, and any credentials issued for their access should grant the minimum access necessary, then revoked immediately upon completion of their work.



Records retention laws affect how long data must be maintained. These requirements must be considered to protect rights under the Public Information Act.

Computers might need to be backed up before disposal.

Sanitation and Disposal of Storage Media


The media containing information (hard drives both portable and fixed, USB/flash drives, CD/DVDs, internal RAM/ROM memory cards, discs of all kinds) should be handled carefully when no longer needed. Simply deleting files through the user interface is rarely effective.


Best Practices:

- In old desktops and laptops, hard drives should be erased by completely reformatting them where possible, or else erased with a physical erasure device or hard drive eraser software
- Before being sent on, hard drives should be removed and destroyed where possible from computers as well those in copiers, printers, and scanners, which can retain data they process for years
- Follow manufacturer instructions for reformatting the memory of devices such as phones, tablets, and other peripherals
- Phones and other cellular-enabled devices should have SIM cards removed and destroyed in addition to wiping memory
- Paper records in the workplace should be handled safely and disposed of in protected receptacles
- Reputable, professional services should be contracted for record destruction if not done in-house
- Writable portable media should be erased following manufacturer instructions
- Non-writable media should be physically destroyed

Network Level Security







4 Main Pillars of Cyber Security

[Network Level Pillar]

The Network Level is becoming all-encompassing as **computers no longer operate on an “island”**, and computers are becoming connected in ways most users do not expect.

Potential exposures to your organization:

- Anti-virus, anti-spyware or anti-malware software or firewalls are not effective
- Daily full system scans are not performed to find, quarantine and remove malicious agents from your network before damage is done
- Off-site backups are not maintained
- Lack of administrator controls of networks

www.dcsdq.com

IT staff face many challenges in defending our network. These are some of the issues that can result in problems for organizations.



Review any procedures with supervisors about notifying IT about staff changes.

What is the process when an employee leaves or employment is terminated? Are all the systems that a former employee used still accessible?

This discussion will depend upon what your organization's IT policies are. It is an opportunity to understand why your organization has these processes.

Network Protection

Steps that need to be taken to protect computer networks, whether connected to the internet or not. These are typically managed by IT staff, but users should know key elements:

- Enable user authentication against an authoritative database under the organization's strict control. This system involves the IT professionals setting up and maintaining a list of authorized users.
- Manage roles and permissions set on user accounts and groups and apply those settings to folders and files within a file system.
- User policies set on individual users.
- Wireless security in public and private should be handled carefully. Connections should only be made to known networks, and never free, password-less ones.
- Wherever possible, employ secure connections such as Secure Shell (SSH) or Virtual Private Network (VPN).

Internet Level Security



DCS
DYNAMIC COMPUTING
SERVICES CORPORATION

4 Main Pillars of Cyber Security

[Internet Level Pillar]

Potential exposures to your organization:

- Almost all devices are now capable of connecting to the internet but there are few controls in some organizations to control how they are connected
- Public wi-fi is used continuously without any concern for potential issues
- Administrators do not control or limit access to the internet
- Work provided devices are used away from work extensively
- Employees are not aware of potential issues and training is not provided

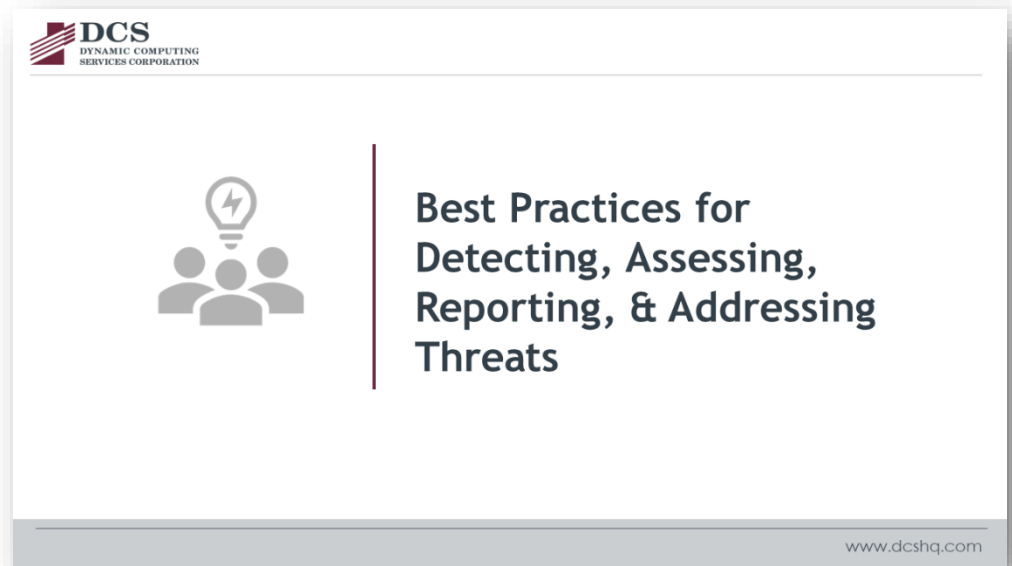
www.dcsdq.com

When connected to the internet, attacks can come through many paths. Many attacks succeed because a user opens the door for them. This slide lists potential issues.

In later sections, we will discuss:

- Protecting you and computers from online threats
- Phishing and social engineering
- Understanding how web browsers work and the warnings they can provide
- Recognizing secure versus unsecure connections
- How to protect you against malware and viruses and what you should do if your device gets infected.

Understanding Threats



Now we shift to learning about cyber threats:

- What is a threat?
- Who are “threat actors”?
- How to detect a threat?
- What are the options to take when there is a threat?

What Is A Threat?



Meaning Of Threat

Threat is the potential targeting of a network or system in an attempt to damage, harm or disrupt its capability to operate. This targeting can potentially impact the confidentiality, integrity and availability of the organization's data.

www.dcsdq.com

Simply put, a threat to information security can be defined as a risk of intrusion or disclosure of confidential information to unauthorized people.


An organization's data has three aspects to consider:

- Confidentiality - the data should be accessible only by authorized users
- Integrity - the data should be accurate
- Availability - the data should be accessible when needed

Common threats include:

- Theft of confidential, proprietary, or sensitive information
- Modification of existing data, and the compromise of how that data is collected, processed, and stored
- Unauthorized access allowing an external user to gain control of a system to block access to data

Who or What Causes the Problem?



What is a “Threat Actor” and What Are Their Goals?

A threat actor is **anyone who tries to exploit vulnerabilities** in an organization’s systems or users.

- Profit, financial or otherwise
- Damaging the victim, financially or otherwise
- Damaging the reputation of the victim gathering data that might be used in future attacks
- Gathering data that might be traded or sold to other actors
- Curiosity or malice

www.dcsdq.com

A threat actor is anyone who tries to exploit vulnerabilities in an organization’s systems or users. It does not matter how sophisticated the attack is or how far it goes. Their motivations and goals can range widely.

They might include:

- Profit, financial or otherwise
- Damaging the victim, financially or otherwise
- Damaging the reputation of the victim (defacing a website, using an email account as a source of spam or malware leading to other attacks, or causing mail from that organization to be blacklisted)
- Gathering data that might be used in future attacks (an attacker might start with an initial round of information gathering, leading to a more technically sophisticated attack later)
- Gathering data that might be traded or sold to other actors
- Curiosity or malice (many attackers start out simply, and try to take actions simply because they can)



It is important to remember that there need not be a particular reason why an attack was made, though understanding the potential attacks allows better defense to be designed. Also, realize that value can be found in all sorts of data. Users might not understand why it is important to keep top financial staff confidential, but to a threat actor those names can then be targeted with attacks to try to gain financial benefit. It's easier to try to get a wire sent if you know who the CFO is and then claim to be the CFO or direct an action in the CFO's name.

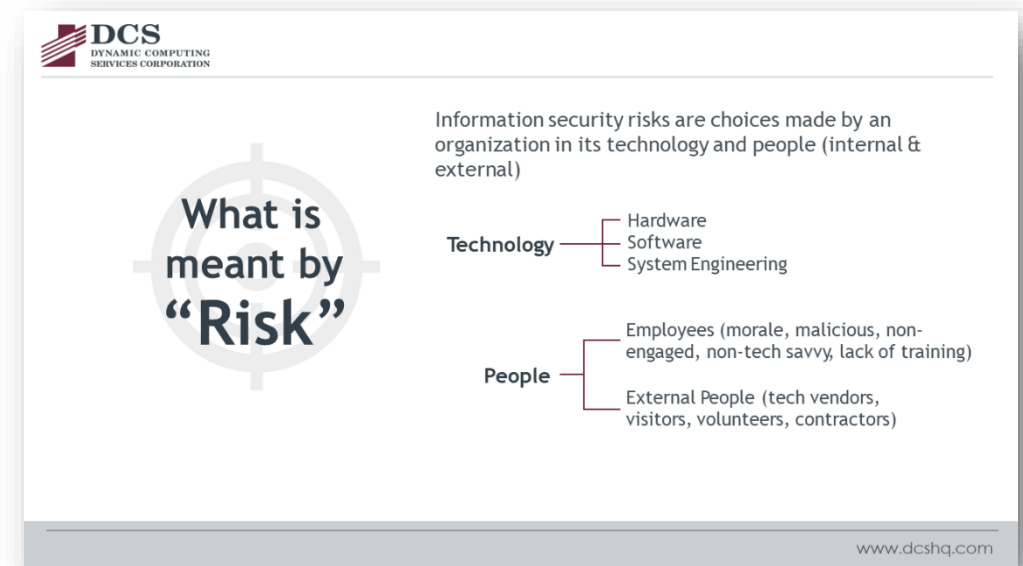


Consider This

The idea of a hacker sitting in a dark room deftly finding cracks in firewalls and guessing passwords is still valid, but just as often these days the door is opened for them by unsuspecting users. **Malware sent in infected email attachments still work**, despite the best efforts of anti-virus software companies to stamp it out. Often that is not needed, however. An email containing a link to a website inviting the user to log in to receive an invoice or other enticement is just as likely to succeed by harvesting that user's username and password as someone with advanced technical skill sneaking in through an arcane software vulnerability.

www.dcsdq.com

Cyber Risk



Information security risks are defined by choices made by an organization in its technology and personnel. The goals of the organization to protect its systems and data against the goals of potential attackers require decisions to be made in view of the needs of its users, usually for accessibility.

For example, the modern office today is highly connected to the internet. Email, websites, file transfer systems, cloud storage, and Software-as-a-Service (SaaS) providers require clear connections to the outside world. Complicating things is that access must be accommodated on many different devices and from any location. These connections thus create potential porousness in defenses. An organization's data can be made much safer if connections to the internet were not allowed. However, that would greatly impact user productivity and likely that data's utility. Most organizations will accept the risk of connecting to the internet in favor of its ease of use.



In 2017, Equifax was hacked, impacting 143 million U.S. consumers. Data included social security numbers, birth dates, addresses, and some drivers' license numbers.


How did this happen? The reports are that the company failed to implement a patch on a part of the company's website.

<https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html>

Does your organization have any computers that are rarely used? Make sure they get regular updates and that your personal computers are updated too.

There are risks of inadequate user knowledge and having dependence on manufacturers of the hardware and software. The news frequently carries stories of devices with vulnerabilities that were previously unknown or, worse, known but left untended by a user or the IT department. When a vulnerability is found in Windows, for example, Microsoft will send out a patch as part of its regular round of updates. If the risk is deemed to be an emergency, they can push one out sooner. But it is incumbent on the user or, preferably, the IT department, to ensure it is applied in a timely manner.

Attacks



What is meant by “Attack”

Attacks on information security can be defined as any **attempt to gain access or control** of an organization's **data or information systems**, no matter what the level of sophistication

Types of Attacks can Include

- Emails
- Phone Calls
- Texts
- USB Drives / Flash drives
- Internet of Things
- Letter

www.dcsdq.com

Attacks on information security can be defined as any attempt to gain access or control of an organization’s data or information systems, no matter what the level of sophistication. Attacks can be simple emails or even phone calls, emails with malware attached, or full-scale electronic attack on a system’s points of access.



*See also: Phishing:
Doing Your Part
and Red Flags
Handout*

Recognizing Common Attacks





Types of Tactics Used in an Attack

- Phishing
- Spear Phishing
- Social Engineering
- Whaling

- Malware
- Ransomware
- Vishing (voice phishing)

www.dcsdq.com

Common attacks include impersonation, phishing and its variants, social engineering, and malware sent via email or other means.

One of the simplest attacks, and one that remains curiously effective, is simple impersonation of a user authorized to make financial payments. A common trick is to create an email on a free service such as Gmail or Hotmail, in the name of the CFO or other person authorized to send a wire. The sender claims to be on vacation and to excuse the personal email, but he or she cannot access work mail. It's suddenly a priority to send a payment and provide wiring instructions.

It is important to note that impersonation attacks are not limited to email. Bold attackers might call on the phone, for example, counting on the user to not recognize a voice or question directives.

Imitation is not limited to employees of the organization. Another common attack, again either with a throwaway email account or a real, compromised account, is to impersonate a vendor and send out messages with "new wiring instructions" so that the next time a bill to that vendor must be paid, the funds will be sent to the attacker's account.

Additional resource: www.onguardonline.gov

Types of Tactics Used in an Attack



Sometimes the link is a word or a phrase, but you can determine the destination of the link by using your mouse pointer and not clicking.

Phishing is the attempt to acquire information such as usernames, passwords, and credit card numbers by pretending to be another entity such as a social website, financial institution, or IT administrator.

The email or message might contain nothing other than a sentence or two and a link to an outside website. The link might be disguised, as the text displayed can be different from the destination encoded in the link. Placing a mouse-pointer on the link without clicking will display the destination of the link in a floating box directly above the link or in the lower left corner of the window. On mobile devices, there may be other ways to display the link without clicking. Users should try to understand how to read the link and decide if it is valid. Often the destination of the link might seem harmless or safe; no software is downloaded, or other intrusive action taken. But a message is shown that in order to access the document the user should log in with his or her username and password.

Often the landing pages of services like Gmail or Office 365 are imitated, including logos and other visual cues. What lies beyond that page is often nothing, or some random document. That is irrelevant, but the important information was already stolen, the user's login credentials. In certain environments, such as organizations that have cloud services like Google or Office365 to provide authentication and authorization across many systems beyond email, a username and password(s) can be keys to the kingdom.

Spear Phishing is a phishing email targeted at a specific individual or department within an organization that appears to be from a trusted source.

Whaling is a phishing attempt that targets high-ranking executives at major organizations.

Vishing is a type of phishing attack conducted by phone, utilizing voice messages to potentially steal protected information.



Quishing is a phishing method using QR (Quick Response) codes. QR codes encode information into two-dimensional barcodes which can be scanned by a QR reader. Malicious actors can generate fake QR codes which direct individuals to fraudulent or infected websites or cause someone to unwittingly download malware or harmful apps.

QRLJacking is a specialized form of quishing targeting Quick Response Login (QRL) systems. Hackers distribute a modified version of a legitimate QR code from a website or app. Since QRL is the QR-based method for user authentication, any account utilizing QRL but lacking multi-factor authentication is exposed.

Smishing is an SMS phishing attempt where attackers try to deceive someone into disclosing personal or financial information, clicking rogue links, or installing malware.

Social engineering applies to any kind of contact intended to gain information or access through non-technical means. It might come through email but also through phone calls, instant message, social media, or any other avenue of communication. When a user gets a call from an unknown person and through possibly pleasant conversation reveals key information about the organization that can be used later.

Ransomware is defined as vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. Annual ransomware costs are estimated to be \$11.5 billion by 2019.

Malware, a term covering software with many names like viruses, trojans, worms, backdoors, spyware, and so on, is very common and destructive. While there are many reputable companies doing excellent work to combat it, it is always true that some get through, especially new formulations that have not yet been recognized.

The risk of lack of user knowledge in how to handle attachments comes into play. No attachment should be delivered to an inbox without scanning for viruses, and a user should not open a document without scanning it again.



*See also: Phishing:
Do Your Part and
Red Flags Handout*



Recognizing Common Attacks

Malware, covering software with many names like viruses, trojans, worms, backdoors, spyware, and so on, is very common and pernicious. While there are many reputable companies doing excellent work to combat it, it is always true that some get through, especially new formulations that have not yet been recognized. **The risk of user aptitude in how to handle attachments comes into play.** No attachment should be delivered to an inbox without scanning, and a user should not open a document without scanning it again.

www.dcsdq.com

Identifying a Phishing Email





Top 10 Tips for Identifying a Phishing Email

1. The message contains a mismatched URL (Uniform Resource Locator)
2. The URL contains a misleading domain name (website name)
3. The message contains poor spelling and/or grammar
4. The message asks for personal information
5. The offer seems too good to be true
6. You didn't initiate the action
7. You're asked to send or provide money or payment
8. The message includes unrealistic threats
9. Something just doesn't look right
10. The email includes an embedded link or attachment that you are asked/tempted to open

www.dcsdq.com

Examples:

Tip #2: Instead of bankofamerica.com the phishing email has bankofamerca.com

Tip #8: Email says someone “knows what you did” and your laptop camera can prove it.

Beyond email, scammers have other techniques.

- Phishing can be tried through other means including text messages, phone calls, fax, or even in person.
- Malware often spreads through contact lists, so it's more likely to come from someone you know.
- If you get a suspicious message, find a phone number to call the sender. Do not assume any number in the email or signature is genuine.
- It may be hard, but caution in any electronic communication should be the default.

QR code Precautions

All the safety measures you would normally exercise such as protecting personal and financial information, utilizing multi-factor authentication, and general awareness should continue to be applied when using QR codes. There are additional measures which pertain specifically to QR code use.

- **Trust the QR source:** Because QR codes are not human readable, it is of the highest importance to confirm their authenticity and to trust the source. If a QR code appears legitimate and is from a colleague, check with them directly to ensure authenticity. For businesses, visit the official website. When in doubt, treat the QR code as untrusted.
- **Reputable QR code reader:** If you use a third-party app instead of the manufacturer's option for scanning QR codes, make certain it's from a trustworthy group or developer. A malicious app can both be malware and infect a device with malware.
- **URL Preview:** If you have the capability to preview a link beforehand in the QR reader, take the time to check that the destination is what you expect before accessing the link.

Additional resource:

<https://www.malwarebytes.com/cybersecurity/basics/quishing>

Responding to Attacks



Responding To and Reporting Common Attacks

www.dcsdq.com



Responding to an Attack

The common thread to all the attacks outlined previously is the reliance on the user not to question or verify the actions requested. The internet was built on trust, with all the threats present today not even imagined when much of the technology at its core was created. Thus, **responsibility falls on the users and organization** to employ a sustained, suspicious vigilance in any contact.

The most powerful key in any security system is the “delete” key. When a user receives **an email that is even a little suspicious, deleting it is usually the best course of action.** Where possible, verification by calling a known phone number is best. The email might contain a phone number to call in case of questions, but better for the user to find a number independently if not already known.

www.dcsdq.com

The common thread to all the attacks outlined previously is the reliance on the user not to question or verify the actions requested. The internet was built on trust, with all the threats present today not even imagined when much of the technology at its core was created. Thus, responsibility falls on the users and organization to employ a sustained, suspicious vigilance in any contact.



Responding to an Attack

Many organizations have an IT department, whether a dedicated, in-house team or an outside contractor; and they should be utilized as a resource for validation of suspicion. Any IT professional will say that it's better to be asked a thousand questions about benign material than to have to eradicate one rampant virus.

Management should be sensitive to user questions and doubts. Without a full-time staff, management should **develop methods for reporting and tracking threat detection**. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

www.dcsdq.com



Responding to an Attack

Attackers might send out a million phishing messages a day with virtually no cost. **Failure to recognize** even one of these **attacks can yield thousands of dollars** to the **attackers and a blow to the reputation** of the organization, not to mention the employee.

www.dcsdq.com

The most powerful key in any security system is the “delete” key. When a user receives an email that is even a little suspicious, deleting it is usually the best course of action. Where possible, verification by calling a known phone number is best. The email might contain a phone number to call in case of questions, but it is better for the user to find a number independently if not already known.



Many organizations have an IT department, whether a dedicated, in-house team or an outside contractor, and they should be utilized as a resource for validation of suspicion. Any IT professional will say that it's better to be asked a thousand questions about benign material than to have to eradicate one rampant virus.

Management should be sensitive to user questions and doubts. Without a full-time staff, management should develop methods for reporting and tracking threat detection. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

Training should be provided to users to identify risks and how to handle them, and that training should be repeated and refined, with periodic testing and review. Attackers might send out a million phishing messages a day with virtually no cost. Failure to recognize even one of these attacks can yield thousands of dollars to the attackers and a blow to the reputation of the organization, not to mention the employee.

Reporting Attacks



Your organization should have a person designated to receive and act upon reports.



Reporting

Users should be aware of how to identify, respond to, and report on threats to information security and suspicious activity

- **Internal Reporting**
All suspicious activity should be reported according to your internal policy
- **External Reporting**
Contact all involved parties (contractors, vendors)
- **Cyber crime must be reported to law enforcement**

www.dcsdq.com

Acknowledgement and Citation [2]

AI in Cyber Security

Artificial intelligence (AI) has been enhancing cyber security tools for years. For example, machine learning tools have made network security, anti-malware, and fraud-detection software more potent by finding anomalies much faster than human beings. However, AI has also posed a risk to cyber security. Brute force, denial of service (DoS), and social engineering attacks are just some examples of threats utilizing AI.

The risks of artificial intelligence to cyber security are expected to increase rapidly with AI tools becoming cheaper and more accessible. For example, you can trick ChatGPT into writing malicious code or a letter from Elon Musk requesting donations,

You can also use a number of deepfake tools to create surprisingly convincing fake audio tracks or video clips with very little training data. There are also growing privacy concerns as more users grow comfortable sharing sensitive information with AI.

Read this in-depth guide for more on:

1. AI Definition.
2. Artificial intelligence risks.
3. AI in cyber security.
4. AI and privacy risks.

What is AI: Artificial Intelligence

AI, or Artificial Intelligence, refers to the development of computer systems that can perform tasks and make decisions that typically require human intelligence. It involves creating algorithms and models that enable machines to learn from data, recognize patterns, and adapt to new information or situations.

In simple terms, AI is like teaching computers to think and learn like humans. It allows machines to process and analyze large amounts of data, identify patterns or anomalies, and make predictions or decisions based on that information. AI can be used in various applications, such as image and speech recognition,

natural language processing, robotics, and cybersecurity, to name a few.

Overall, AI aims to mimic human intelligence to solve complex problems, automate tasks, and enhance efficiency and accuracy in different fields.

Machine learning and deep learning

Machine learning (ML) is a commonly used subset of AI. ML algorithms and techniques allow systems to learn from data and make decisions without being explicitly programmed.

Deep learning (DL) is a subset of ML that leverages artificial computational models inspired by the human brain called neural networks for more advanced tasks. ChatGPT is an example of AI that uses ML to understand and respond to human-generated prompts.

Narrow AI and artificial general intelligence

All types of AI are considered Narrow AI. Their scope is limited, and they're not sentient. Examples of such AI are voice assistants, chatbots, image recognition systems, self-driving vehicles, and maintenance models.

Artificial general intelligence (AGI) is a hypothetical concept that refers to a self-aware AI that can match or even surpass human intelligence. While some experts estimate that AGI is several years or even decades away, others believe that it's impossible.

What is generative AI?

Generative AI refers to a subset of artificial intelligence techniques that involve the creation and generation of new content, such as images, text, audio, or even videos. It involves training models to understand patterns in existing data and then using that knowledge to generate new, original content that resembles the training data.

One popular approach to generative AI is the use of generative adversarial networks (GANs). GANs consist of two neural networks: a generator network and a discriminator network. The generator network creates new content, while the discriminator network evaluates and distinguishes between the generated

content and real content. The two networks work in a competitive manner, with the generator attempting to produce content that the discriminator cannot distinguish from real data.

Generative AI has applications in various domains. For example:

1. **Image Generation:** Generative AI can be used to generate realistic images, such as creating photorealistic faces, landscapes, or even entirely new objects that do not exist in the real world.
2. **Text Generation:** Generative models can be trained to generate coherent and contextually relevant text, which can be used for tasks like chatbots, content creation, or language translation.
3. **Music and Audio Generation:** Generative AI can create new musical compositions or generate realistic sounds and voices.

While generative AI has many positive applications, there are also concerns about its potential misuse, such as generating fake content or deepfake videos that can be used to deceive or manipulate people. Ethical considerations and responsible use of generative AI are important factors to address these risks.

In the realm of cybersecurity, generative AI can be both a tool and a challenge. It can be used for generating realistic synthetic data to train models and improve security measures, but it can also pose risks when used for malicious purposes, such as generating convincing phishing emails or deepfake social engineering attacks. It highlights the importance of developing robust defenses and detection mechanisms to mitigate potential threats.

What are the risks of AI in cyber security

Like any technology, AI can be used for good or malicious purposes. Threat actors can use some of the same AI tools designed to help humanity to commit fraud, scams, and other cybercrimes.

Let's explore some risks of AI in cyber security:

1: Cyber attacks optimization

Experts say that attackers can use generative AI and large language models to scale attacks at an unseen level of speed and complexity. They may use generative AI to find fresh ways to undermine cloud complexity and take advantage of geopolitical tensions for advanced attacks. They can also optimize their ransomware and phishing attack techniques by polishing them with generative AI.

2: Automated malware

An AI like ChatGPT is excellent at accurately crunching numbers. According to Columbia Business School professor Oded Netzer, ChatGPT can already “write code quite well.”

Experts say that in the near future, it may help software developers, computer programmers, and coders or displace more of their work.

While software like ChatGPT has some protections to prevent users from creating malicious code, experts can use clever techniques to bypass it and create malware. For example, one researcher was able to find a loophole and create a nearly undetectable complex data-theft executable. The executable had the sophistication of malware created by a state-sponsored threat actor^[3].

This could be the tip of the iceberg. Future AI-powered tools may allow developers with entry-level programming skills to create automated malware, like an advanced malicious bot. So, what are malicious bots? A malicious bot can steal data, infect networks, and attack systems with little to no human intervention.

[3] [https://www.foxnews.com/tech/ai-created-malware-sends-shockwaves-cyber security-world](https://www.foxnews.com/tech/ai-created-malware-sends-shockwaves-cyber-security-world)

3: Physical safety

As more systems such as autonomous vehicles, manufacturing and construction equipment, and medical systems use AI, risks of artificial intelligence to physical safety can increase. For example, an AI-based true self-driving car that suffers a cyber

security breach could result in risks to the physical safety of its passengers. Similarly, the dataset for maintenance tools at a construction site could be manipulated by an attacker into creating hazardous conditions.

AI privacy risks

In what was an embarrassing bug for OpenAI CEO Sam Altman, ChatGPT leaked bits of chat history of other users.

Although the bug was fixed, there are other possible privacy risks due to the vast amount of data that AI crunches. For example, a hacker who breaches an AI system could access different kinds of sensitive information.

An AI system designed for marketing, advertising, profiling, or surveillance could also threaten privacy in ways George Orwell couldn't fathom. In some countries, AI-profiling technology is already helping states invade user privacy.

Stealing AI models

There are some risks of AI model theft through network attacks, social engineering techniques, and vulnerability exploitation by threat actors such as state-sponsored agents, insider threats like corporate spies, and run-of-the-mill computer hackers. Stolen models can be manipulated and modified to assist attackers with different malicious activities, compounding artificial intelligence risks to society.

Data manipulation and data poisoning

While AI is a powerful tool, it can be vulnerable to data manipulation. After all, AI is dependent on its training data. If the data is modified or poisoned, an AI-powered tool can produce unexpected or even malicious outcomes.

In theory, an attacker could poison a training dataset with malicious data to change the model's results. An attacker could also initiate a more subtle form of manipulation called bias injection. Such attacks can be especially harmful in industries such as healthcare, automotive, and transportation.

Impersonation

You don't have to look further than cinema to see how AI-powered tools are helping filmmakers trick audiences. For example, in the documentary *Roadrunner*, the late celebrity chef Anthony Bourdain's voice was controversially created with A.I.-generated audio and easily tricked viewers. Similarly, the veteran actor, Harrison Ford, was convincingly de-aged by several decades with the power of artificial intelligence in *Indiana Jones and the Dial of Destiny*.

An attacker doesn't need a big Hollywood budget to pull off similar trickery. With the right footage, anyone can make deepfake footage by using free apps. People can also use free AI-powered tools to create remarkably realistic fake voices trained on mere seconds of audio.

So it should come as no surprise that AI is now being used for virtual kidnapping scams. Jennifer DeStefano experienced a parent's worst nightmare when her daughter called her, yelling and sobbing. Her voice was replaced by a man who threatened to drug her and abuse her unless paid a \$1 million ransom.

The catch? Experts speculate the voice was generated by AI. Law enforcement believes that in addition to virtual kidnapping schemes, AI may help criminals with other types of impersonation fraud in the future, including grandfather scams.

Generative AI can also produce text in the voice of thought leaders. Cybercriminals can use this text to run different types of scams, such as fraudulent giveaways, investment opportunities, and donations on mediums like email or social media platforms like Twitter.

More sophisticated attacks

As mentioned, threat actors can use AI to create advanced malware, impersonate others for scams, and poison AI training data. They can use AI to automate phishing, malware, and credential-stuffing attacks. AI can also help attacks evade security systems like voice recognition software in attacks called adversarial attacks.

Reputational damage

An organization that utilizes AI can suffer reputational damage if the technology malfunctions or suffers a cyber security breach, which results in data loss. Such organizations may face fines, civil penalties, and deteriorating customer relationships.

How to protect yourself from the AI risks

While AI is a powerful tool, it can present some cyber security risks. Both individuals and organizations must take a holistic and proactive approach in order to use the technology safely.

Here are some tips that can help you mitigate the risks of AI:

1: Audit any AI systems you use

Check the current reputation of any AI system you use to avoid security and privacy issues. Organizations should audit their systems periodically to plug vulnerabilities and reduce AI risks. Auditing can be done with the assistance of experts in cyber security and artificial intelligence who can complete penetration testing, vulnerability assessments and system reviews.

2: Limit personal information shared through automation

More people are sharing confidential information with artificial intelligence without understanding the AI risks to privacy. For example, staff at prominent organizations were found putting sensitive company data in ChatGPT. Even a doctor submitted his patient's name and medical condition in the chatbot to craft a letter, not appreciating the ChatGPT security risk.

Such actions pose security risks and breach privacy regulations like HIPAA. While AI language models may not be able to disclose information, conversations are recorded for quality control and are accessible to system maintenance teams. That's why it's best practice to avoid sharing any personal information with AI.

3: Data security

As mentioned, AI relies on its training data to deliver good outcomes. If the data is modified or poisoned, AI can deliver unexpected and dangerous results. To protect AI from data poisoning, organizations must invest in cutting-edge encryption,

access control, and backup technology. Networks should be secured with firewalls, intrusion detection systems, and sophisticated passwords.

4: Optimize software

Follow all the best practices of software maintenance to protect yourself from the risk of AI. This includes updating your AI software and frameworks, operating systems, and apps with the latest patches and updates to reduce the risk of exploitation and malware attacks. Protect your systems with next-generation antivirus technology to stop advanced malicious threats.

In addition, invest in network and application security measures to harden your defenses.

5: Adversarial Training

Adversarial training is an AI-specific security measure that helps AI respond to attacks. The machine learning method improves the resilience of AI models by exposing them to different scenarios, data, and techniques.

6: Staff training

The risks of AI are quite broad. Consult with experts in cyber security and AI to train your employees in AI risk management. For example, they should learn to fact-check emails that may potentially be phishing attacks designed by AI. Likewise, they should avoid opening unsolicited software that could be malware created by artificial intelligence.

7: Vulnerability management

Organizations can invest in AI vulnerability management to mitigate the risk of data breaches and leaks. Vulnerability management is an end-to-end process that involves identifying, analyzing, and triaging vulnerabilities and reducing your attack surface related to the unique characteristics of AI systems.

8: AI incident response

Despite having the best security measures, your organization may suffer an AI-related cyber security attack as the risks of artificial intelligence grow. You should have a clearly outlined incident response plan that covers containment, investigation, and remediation to recover from such an event.

The flip side: How AI can benefit cyber security

Industries of different sizes and sectors use AI to enhance cyber security. For example, all types of organizations worldwide use AI to authenticate identities, from banks to governments. And the finance and real estate industries use AI to find anomalies and reduce the risk of fraud.

Here is more on how AI benefits cyber security:

1: Cyber threat detection

Sophisticated malware can bypass standard cyber security technology by using different evasion techniques, including code and structure modification. However, advanced antivirus software can use AI and ML to find anomalies in a potential threat's overall structure, programming logic, and data.

AI-powered threat detection tools can protect organizations by hunting these emerging threats and improving warning and response capabilities. Moreover, AI-powered endpoint security software can shield the laptops, smartphones, and servers in an organization.

2: Predictive models

Cybersecurity professionals can go from a reactive to a proactive posture by utilizing generative AI. For example, they can use generative AI to create predictive models that identify new threats and mitigate risks.

Such predictive models will result in:

- Faster threat detection
- Time savings
- Cost reduction
- Improved incident response
- Better protect from risks

3: Phishing detection

Phishing emails are a significant threat vector. With little risk, threat actors can use phishing expeditions to steal sensitive information and money. Moreover, phishing emails are becoming more challenging to differentiate from real emails.

AI can benefit cyber security by enhancing phishing protection. Email filters that utilize AI can analyze text to flag emails with suspicious patterns and block different types of spam.

4: Identifying bots

Bots can harm or take down networks and websites, negatively impacting an organization's security, productivity, and revenue. Bots can also take over accounts with stolen credentials and help cybercriminals engage in fraud and scams.

Software that leverages machine learning-based models can analyze network traffic and data to identify bot patterns and help cyber security experts negate them. Network professionals can also use AI to develop more secure CAPTCHA against bots.

5: Securing networks

Attackers can exfiltrate data or infect systems with ransomware after breaching a network. Detecting such threats early is critical. AI-based anomaly detection can scan network traffic and system logs for unauthorized access, unusual code, and other suspicious patterns to prevent breaches. Moreover, AI can help segment networks by analyzing requirements and characteristics.

6: Incident response

AI can boost threat hunting, threat management, and incident response. It can work around the clock to respond to threats and take emergency action, even when your team is offline. In addition, it can reduce incident response times to minimize harm from an attack.

7: Mitigate insider threats

Insider threats must be taken seriously because they can cost an organization revenue, trade secrets, sensitive data, and more. There are two types of insider threats: malicious and unintentional. AI can help stop both types of insider threats by identifying risky user behavior and blocking sensitive information from leaving an organization's networks.

8: Strengthen access control

Many access control tools use AI to improve security. They can block logins from suspicious IP addresses, flag suspicious events, and ask users with weak passwords to change their login credentials and upgrade to multi-factor authentication.

AI also helps authenticate users. For example, it can leverage biometrics, contextual information, and user behavior data to accurately verify the identity of authorized users and mitigate the risk of misuse.

9: Identify false positives

False positives can be exhausting for IT teams to manage. The sheer volume of false positives can result in mental health challenges. They can also force teams to miss legitimate threats. The volume of false positives can be reduced, though, with cyber security tools that use artificial intelligence to improve threat detection accuracy. Such tools can also be programmed to automatically manage low-probability threats that consume a security team's time and resources.

10: IT staffing efficiency and costs

Many small to medium-sized businesses can't afford to invest in a large in-house cyber security team to manage increasingly sophisticated threats around the clock. However, they can invest in AI-powered cyber security technology that works 24/7 to offer continuous monitoring, improve efficiency and reduce costs. Such technology can also scale with the growth of a company cost-effectively.

In addition, AI improves staff efficiency because it doesn't tire. It offers the same quality of service at all hours of the day, reducing the risk of human error. AI can also manage significantly more data than a human security team.

^[2] Full acknowledgement to Malwarebytes for the preceding section. Content is solely theirs from the AI in Cyber Security: Risks of AI webpage at: <https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security>

Working Remote Best Practices



*See also: NCCoE
Telework Security
Overview & Tip
Guide Handout*

Many organizations are increasingly providing employees flexible work methods including the option to work remotely. Work may be exclusively performed remotely, or it may be hybrid, a mix of both onsite and remote.

However, working remotely does introduce additional risks for both the organization and remote workers.

The following are some **Best Practices** for working remotely.


- Understand your organization's remote work policies and be aware of updates or changes
- Protect device communications between your router or Wi-Fi by implementing strong passwords and security protocols
- Use your organization's VPN or remote access gateway and consider using your own VPN to further secure the connection
- If you are using a personal device, not issued by your organization, enable security features such as passwords and/or biometrics to limit unauthorized access
- Keep all devices up to date with the latest patches and security updates
- Only install trusted software from trusted sources
- Use an antivirus program
- Only visit trusted websites and, when available, employ Multi-Factor Authentication (MFA), for additional login security
- Report any unusual or suspicious activity to your organization immediately

Additional resources:


www.cio.gov/cybersecurity-experts-provide-remote-work-best-practices/
us.norton.com/blog/emerging-threats/working-from-home-due-to-coronavirus

Training





Provide external and internal stakeholders with tools needed to ensure **reliability, usability, and security**



**Training
And Policies**

- Policies that ensure information security
- Vetting of internal and external stakeholders
- Employee Training

Programs

- ✓ Meets Texas Government Code Requirements
- ✓ Awareness Based Training Internal
- ✓ Policy Training
- ✓ Ongoing Training (new exposures as identified)

www.dcsdq.com

Management should be sensitive to user questions and doubts. Without a full-time staff, management should develop methods for reporting and tracking threat detection. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

Training should be provided to users to identify risks and how to handle them, and that training should be repeated and refined, with periodic testing and review. Attackers might send out a million phishing messages a day with virtually no cost. Failure to recognize even one of these attacks can yield thousands of dollars to the attackers and a blow to the reputation of the organization, not to mention the employee.

Conclusion



Before taking the Assessment test, re-read the Cyber Security Awareness Handout as a refresher.

DCS
DYNAMIC COMPUTING
SERVICES CORPORATION

Conclusion

- Testing/Assessment of Knowledge (Corrected to 100%)
- Record of Completion (Personnel File)

www.dcsHQ.com

The concludes the Cyber Security Awareness course. Please take the Assessment test and provide it to your organization.

DCS
DYNAMIC COMPUTING
SERVICES CORPORATION

Free Resources for Public Entities

- All governmental entities have free access to: <https://www.cisecurity.org/ms-isac/>

www.dcsHQ.com

^[1] Program based on, and acknowledgement to, Texas Municipal League Intergovernmental Risk Pool