



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Part 3 – Slide 1

Welcome to the Department of General Services Information Security and Privacy Awareness training.

This training is provided to you by the DGS Information Security Office (ISO).

You may contact our office via email, phone or mail.

For more information about Information Security, please visit our website at ISO.DGS.CA.GOV



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 2

Agenda

This is the third of three presentations included in this year's security awareness training.

In this presentation we will talk about information security and how it relates to you in a practical sense. This presentation is designed to give you real tools and awareness which you can use in your daily work day.

We'll talk about information security best practices covering a wide range of subjects that will help to build your awareness of typical security pitfalls and how to avoid them.

Next we'll talk about security incident management; how to identify if there has been an information security incident and the steps to take if an incident has occurred.

We'll review the security and confidentiality form that must be filled out once the training is completed.

And finally we'll wrap up with information on how to contact the information security office as well as other resources that may be helpful to you.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 3

Security Best Practices

For our discussion of “Security Best Practices” we will be covering four basic topics.

Facility Security – general practices to ensure that our buildings, offices, shops and equipment are safe and secure

Electronic Security takes it one step further in ensuring that the electronic tools we use remain secure.

Acceptable Use addresses some of the activities that are not appropriate in DGS computing environments

And lastly, **Social Engineering** where we as individuals become the most essential link in the chain of information security



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 4

Physical Security

Maintaining good physical security is the first layer of protection in information security.

Physical security includes maintaining secure facilities where work can be done in a safe environment so data loss can be contained or controlled.

Secure computers where data can be created, processed and transmitted with managed security and protection.

And secure devices and media, where electronic data is securely stored and kept safe from data loss or tampering.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 5

Facility Security

By keeping our facilities secure from outsiders, it produces a direct impact on helping ensure our people, systems and data are safe.

This begins with using the DGS ID badge. Being readily identified ensures that only authorized staff is present when working in sensitive areas or with sensitive information.

Once we ensure that only authorized staff is present in our work areas, we can ensure that work areas are properly secured or locked down. Sensitive information should be locked up in secure offices or locked file cabinets when not in use.

Access cards should be issued to each individual employee to allow access to work areas. Keep your access card with you at all times to avoid theft and potential unauthorized access.

Care should be taken when using access cards to enter work areas. Tailgating is the process of allowing another person to follow behind you when accessing a secure area using an access card. Disallowing tailgating ensures that personnel are authorized entry and that work areas remain secure.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 6

Secure Computers

In today's business world, much of the work we do is accomplished on personal computers.

Securing our computers is just as important as locking up our doors and file cabinets. When considering securing computers, it is important to think of it as securing the data that resides within the computer and not simply the computer itself. While a computer may cost several hundred or thousand dollars, the cost is minimal compared to the potential losses that may occur as a result of lost or stolen data.

When leaving your computer unattended, be sure to "lock" your computer. On windows PC's this is done by pressing the ConTRoL, ALT, and DELeTe keys simultaneously, then selecting "lock computer." You can also press the "windows key" and "L" to immediately lock your computer. Locking your computer ensures that other users cannot use your computer while you are away.

If traveling with DGS laptop computers, it is important ensure that your laptop is properly secured within vehicles, hotel rooms or other public places. It is best to treat a laptop computer as you would a large sum of money and protect it accordingly. In vehicles, store laptops out of view within a locked trunk being the best and prior to arrival at your destination. If possible, keep laptops in the hotel safe. If there is no secure storage, then you may find it best to tote your laptop with you.

Lastly, use good password security practices such as changing the password frequently as well as not writing it down.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 7

Secure Devices and Media

Because so much of the data we manage has become so portable, individual users have become data custodians and are responsible for safeguarding data from loss or theft.

Just as we must secure our offices, computers and other data, it is important to properly secure flash drives, smart phones, other data carrying devices as well as paper files. These types of portable media should be properly stored in locked cabinets or offices. Such devices should also be encrypted with password protection if possible to ensure that if the physical device is lost or stolen, the data contained remains secure.

Proper handling of the physical devices goes hand in hand with the proper management of sensitive data. Retired PCs, laptops, and servers headed for surplus property should be inspected for sensitive data and the data removed and the disc drives properly sanitized prior to disposal. This along with proper shredding and disposal of sensitive paper documents prevents data “leakage” through unexpected channels.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 8

Electronic Security

Just as we secure our facilities by using locks, access badges and security staff so we must secure our computers and electronic data.

Because most of our data is stored, managed or transmitted by electronic means, securing these electronic assets is very important.

By using good password security practices, we prevent unauthorized access right at the “front door” of our systems and applications.

Through malware awareness and prevention we ensure that data and systems are kept safe from malicious software and hacking tools.

And with telework and mobile security awareness, we keep our assets safe even on the move.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 9

Password Security

Your account on DGS networks is special. It has been set up for you, for your exclusive use. It has characteristics that help you to get your work done, and establish your online identity in regards to email and access to files and information assets throughout DGS. The primary method that your account or identity is protected is by the password you create on your account. Using a strong, secure password not only helps to protect DGS assets, but ensures that your account and files are kept safe.

Most passwords are cracked by a computer program running many letter combinations at high speed or by someone simply guessing your password. The best defense is to create a password at least eight characters long that includes a few symbols—such as the dollar sign, pound sign, or exclamation point—as well as letters and numbers. Long, complex passwords are harder to break—even for high-speed computer programs—because the number of possible combinations.

Never use personal information such as names of family members, friends or pets. Don't use birthdays, or the names of your favorite sports teams or bands.

Whatever you do, never share your passwords with anyone or allow yourself to be tricked into giving them away. Don't write down your password. Commit it to memory. Change your password according to DGS policy and remember, creating a complex, strong password and protecting its secrecy is critical for protecting DGS information and information systems as well as for protecting your own personal information.

Malware

The leading online threat to your PC is malicious software such as computer viruses, worms, Trojans, and spyware often referred to as malware. In today's environment, most malware now targets stealing your personal information for the purpose of identity theft and cyber crime.

Viruses

Often hidden in what appear to be useful or entertaining programs or e-mail attachments, computer viruses are software programs that are deliberately designed by online attackers to invade your computer, interfere with its operation, and to copy, corrupt or delete your data. These malicious software programs are called viruses because they are designed not only to infect and damage one computer, but to spread to other computers all across the Internet. Most viruses are spread by computer users who pass them along in e-mail to friends and colleagues while worms are more sophisticated and can automatically replicate and send themselves to other computers.

Trojan Horses

Other viruses, called Trojans in honor of the Trojan horse, actually masquerade as beneficial programs while quietly destroying your data and damaging your system.

Spyware

As the name implies, spyware is software that is designed to secretly monitor all of the things you do on your computer, and to either report your behavior to the person who designed the program or to take some action based on that information.

Spyware may bombard you with pop-up ads, collect personal information about you, change your settings or even disable your computer. Most importantly spyware can make it possible for criminals to steal your identity.

Contact the OTR Helpdesk immediately if you believe your DGS PC may be infected with any of these and contact your supervisor or the ISO if you believe that a security incident may have occurred.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 11

Telework and Mobile Security

With telework on the rise many DGS employees are finding themselves working either while mobile or outside the confines of DGS facilities.

Special care should be taken to ensure that you are working securely while teleworking from home, in a remote location, or using mobile devices such as smart phones.

If possible, avoid using public "hotspots" for Internet connections and avoid working with sensitive material in public places to avoid the possibility of "over the shoulder" surfing by passers-by.

If you must access DGS resources via a wireless network, ensure that connections are secure using wireless encryption and try to keep sensitive material access to a minimum.

The basic rule of thumb with mobile security is to let the work you are doing determine the level of protection or security. If you find that you can not properly ensure the security of your work at the mobile or remote location, then it is probably best to conduct your work when you can get to a more secure location.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 12

Appropriate Use

Along with standards for security and privacy, DGS users are subject to standards of acceptable use.

The state reserves the right to monitor any and all usage and authorized users should expect no privacy while accessing DGS information assets.

Incidental personal use of state resources for email or internet is permitted, but such usage must not interfere with normal job performance and must not pose a security risk for the department. Furthermore, DGS assets must not be used for private gain, inappropriate, obscene or illegal activities.

DGS email is intended to be user for authorized business use only. As such, forwarding or sending email containing sensitive or personal information from the DGS e-mail system to external email is prohibited. Creating or forwarding spam messages is prohibited. Also using email to harass or threaten other is prohibited.

All software used by DGS employees is to be installed and managed by IT Services Division. Any unauthorized software will be immediately removed. Any copying of copyrighted material for which DGS does not have an active license is strictly prohibited. Certain software such as hacking tools and peer to peer file sharing software pose a specific security risk and will be immediately removed.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 13

File Sharing and Copyright

Peer to peer software or P2P such as Kazaa, limewire or bittorrent is frequently used to download or share music, movies, and other copyrighted material from the Internet without purchase. Downloading files in this way is illegal, unethical and prohibited on all state owned computers and networks. It can also result in criminal or civil liability charges for illegal duplication and sharing of copyrighted material.

Many P2P applications are easily available, but using unauthorized P2P software goes beyond a legal and ethical issue and becomes a security issue. It provides outsiders with a link into your computer and into the DGS's computer networks. This can result in significant vulnerabilities, including unauthorized access to data and the spread of computer viruses and spyware.

Other common applications while not expressly peer to peer software have peer to peer functionality. Communication software skype, music software itunes and many chat and instant messaging use peer to peer as part of their functionality so its important that all software installed on computers is approved prior to installation.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 14

Social Engineering

Social engineering is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this factor.

No matter how much effort is put in to the technology to secure our resources... it's up to "Maggie" in accounting or her friend, Jeff, dialing in from a remote site to keep the DGS network secured.



Phishing

Phishing is one type of social engineering that uses email or websites to trick you into disclosing personal sensitive information, such as credit card numbers, bank account information, your social security number or passwords. The intention is to steal your identity, commit crimes in your name, or access your organization's computer systems. Phishers try to deceive you by sending emails or pop-ups that appear to be from a legitimate business or organization such as your ISP or bank.

The message might claim that you need to update or validate your account info. It might threaten some dire consequence if you don't respond. The message directs you to a website that *looks* just like a legitimate organization's site, but it is not actually affiliated with the real organization in any way. The bogus site tricks you into giving up your personal information. Responding and providing your bank account information to any of these types of emails places your financial security at great risk. Phishers can steal the money in your bank account, access your other bank accounts and can use your name and banking information to steal your identity.

Avoid being a target for phishers. Never click on links in emails or popup messages if they ask for personal or financial information. If an email appears suspicious, do not open it. Simply delete it. If you must view it, make sure to view the email in plain text if possible. Finally, do not open attachments from suspicious emails.

Legitimate companies do not ask for personal information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine. If you want to check your account status online, type the web address directly into your browser or use your personal bookmark.

For more information on how to identify phishing emails see the DGS ISO website at <http://iso.dgs.ca.gov>.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 16

Internet Hoaxes

Along with phishing, Internet hoaxes are email messages often designed to influence you to forward them to everyone you know.

Hoaxes encourage you to forward email messages by warning of new viruses, promoting moneymaking schemes, or citing fictitious causes. By encouraging mass distribution, hoaxes clog networks and slow down Internet and email services for computer users. A forwarding request can also be part of a hacking attack, intended to bring down computer networks by flooding them with traffic.

By forwarding an email to large groups of other users, you are helping hackers execute their attack. You can limit the effect of email hoaxes by following these security tips: If you are suspicious about an email, perform a quick online search to confirm or expose the message. Many legitimate websites list the latest email hoaxes. If an email request that you forward the message to everyone in your address book, it is probably a hoax and do not forward it.

Hoaxes can often be confirmed quickly with a little investigation. Snopes.com is an Internet site that specializes in tracking and moderating Internet rumor and hoaxes. You may also contact the information security office regarding potential Internet hoaxes.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 17

Identity Theft

Identity theft occurs when someone uses your name, address, social security number, banking information or other identifying information without your knowledge to commit fraud or other crimes. Identity thieves can use the information they obtained to open credit card accounts, take out loans, or drain bank accounts without your knowledge.

Identity theft is a serious problem with extreme consequences for its victims. You are the first line of defense against identity theft. It is important that you take action to minimize your risk. Never give out personal info, especially your social security number without knowing how it will be used. Pay attention to credit card and bank statements for unauthorized activity. Avoid using common names or dates when creating passwords or personal identification or PIN numbers. Pick up your mail promptly. Shred all personal documents and mail that contains sensitive info, especially pre-approved credit card offers.

Do not carry your social security card or passport in your purse or wallet. Order copies of your credit report every year and check them for strange or unauthorized accounts.

Following these guidelines can reduce the chance of someone obtaining your personal information and making you a victim of ID theft.

Social Networks

Social networking sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

All social networks allow you to provide information about yourself and offer some type of way that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest.

Because of this active communication platform, all of the elements of Social Engineering become even easier with Social Networks.

Hackers use phishing and hoax attacks with the goal of gaining access to a user's social network account. Once access is stolen, the hacker can now impersonate the social networker and attempt to attack or social engineer the user's entire social group. This type of social engineering attack is even more effective because the attacker is impersonating a trusted person, and can more easily convince a social networker's group of online friends of whatever they wish.

Most social networking attacks focus on impersonation. Whether for the purpose of extracting money from social groups or destruction of personal reputation or credibility, such online attacks can be potentially devastating to victims and organizations.

As with all other social engineering attacks taking time to use caution and vigilance can avert many of the potential pitfalls involved with social networking



How can you protect yourself?

While social engineering attacks can come from many different directions, and the peril of falling victim to such attacks may be severe it is possible to avoid falling victim to social engineering attacks.

Limit the amount of personal information you post or send - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

Remember that the Internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may and likely will still exist on other people's machines.

Be wary, be skeptical - The Internet makes it easy for people to misrepresent their identities and motives. Don't believe everything you read online. Consider limiting the people who are allowed to contact you. People may post false or misleading information about various topics, including their own identities.

Use strong passwords - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and impersonate you. Use different account names and passwords for the different sites you may visit and do not use your DGS account name and password.

Use and maintain anti-virus software - Anti-virus software recognizes most known viruses and protects your computer against them, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your software up to date.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 20

Security Incident Management

No matter how hard we work in avoiding the pitfalls of information security, sometimes things don't work as planned and data or information assets are lost or otherwise compromised. When this happens, a security incident has taken place.

According to DGS policy, a security incident is any intentional or unintentional event which may result in unauthorized access, loss, disclosure, modification, or destruction of information resources or assets.

For example,

- The theft of a laptop, mobile phone, or briefcase containing personally identifiable information.
- The accidental release of confidential information through a forward of a sensitive email message.
- Visiting of inappropriate web sites
- Or sharing of a DGS user name and password.

These are just a few examples of security incidents that must be reported to the ISO. Failure to report such incidences does not comply with SAM requirements, and can put the department at risk.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 21

Security Incident Management - Reporting

Any suspected, attempted, or actual security incident must be immediately reported.

In the event of a suspected or actual incident an employee must immediately inform their supervisor.

The Supervisor then reports to the ISO. The ISO will determine whether or not an actual security incident has occurred and appropriate actions to take. Once reported within DGS, the ISO reports to the appropriate external departments and manages the incident through the entire reporting process.

The supervisor is also responsible for completing the Security Incident Report Form and submitting it to the ISO within two days.

When in doubt, report it.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 22

Security & Confidentiality Acknowledgement

After completing this training, be sure to print out and complete the Security and Confidentiality Acknowledgement form. The completed form shall be submitted to your supervisor. This form certifies that you have completed the training for this year.

Supervisors will maintain the form in the employee files and ensure the training is entered into ABMS.

Detailed instructions for employees and supervisors are available on the form's instruction sheet.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 23

Statewide Resources

You can find more information about information security as it relates to state business at the California Office of Information Security & Privacy protection and the California Highway patrol computer crime websites.

To find more information about protecting your family and home life online, you can visit the National Cyber Security alliance at staysafeonline.org or the Internet Keep Safe coalition at www.ikeepsafe.org

Links to these resources can be found at the DGS ISO website at iso.dgs.ca.gov



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 3

Slide 24

Thank You

This concludes the Information Security Awareness training for 2009.

For any questions regarding this training presentation or information security issues or incidents, please feel free to contact the information security office directly.

We are located in the Ziggurat Building in West Sacramento

We can be reached by phone at (916)376-3940

By email at dgsinfosec@dgs.ca.gov

Or on the intranet at iso.dgs.ca.gov

TIME: 35 SECONDS
