Security Awareness

Security Awareness - Introduction

Welcome!

Welcome to the Security Awareness training. The safety and security of employees and facilities has always been a priority of CenterPoint Energy.

CenterPoint Energy, (CNP), has a responsibility to protect its resources so we can safely gather, transport, and deliver natural gas and electricity to our customers.

Security Awareness - Introduction

What does Security Awareness mean?

Security awareness is the knowledge and mindset CNP employees possess for protecting themselves, other employees, and the physical and information assets of the company.

Being “security aware” means you understand there is the potential for some people to deliberately or accidentally cause loss or harm to you, your fellow employees or CNP assets.

Security Awareness - Introduction

- provide you with skills and information to ensure data/computer system tasks are kept and performed securely
- clarify our responsibility as an organization for maintaining security
- provide you with tips for keeping CNP facilities and physical assets secure
- help you recognize and respond appropriately to real and potential security concerns

Security Awareness - Topics

Cyber Security

- What is cyber security for CNP
- Common cyber security threats
- Best practices for cyber security

Physical Security

- What is physical security for CNP
- Best practices for physical security

Cyber Security

Cyber Security - Introduction

What is Cyber Security?

Cyber Security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

CNP collects processes and stores a great deal of confidential information on computers and transmits that data across our network to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business, customer and other information.

Cyber Security - Introduction

Cyber Crimes

On December 23, 2015, (4) Ukrainian power companies experienced a cyber-attack that caused power outages which impacted over 225,000 customers in the Ukraine.

The new generations of hackers are programming software to enable the theft of money, data or both.

CenterPoint Energy recognizes the critical role Information Security plays in supporting its business objectives.

DAILY
World • Eco
ht © Daily News XXII
Cyber attack
World's leaders meet to-day to discuss global and terrorism is

Cyber Crime - Common Threats

Malware

Data Leakage

Email

Cyber Crime - Common Threats

Malware

- Malicious software
- Computer viruses
- Worms
- Trojan horses
- Spyware
- Dishonest adware
- Crime ware
- Pop-ups with fake anti-virus software

Cyber Crime - Common Threats

Malware

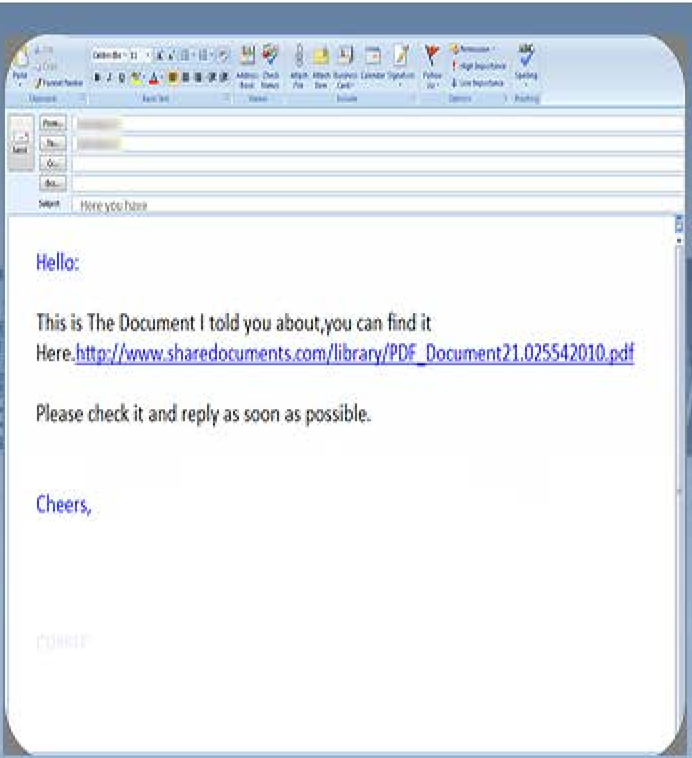
- Untrusted wireless points (hotels, coffee shops, etc.)
- Botnets
- Keylogging

Cyber Crime - Common Threats

Data Leakage

- Unintentional release of secure information to an untrusted environment.
- Loss of data storing devices such as laptops, thumb drives or smart phones
- DLP (Data Loss Prevention) programs

Cyber Crime - Common Threats



Subject: Here you have

Hello:

This is The Document I told you about,you can find it Here.http://www.sharedocuments.com/library/PDF_Document21.025542010.pdf

Please check it and reply as soon as possible.

Cheers,

Email

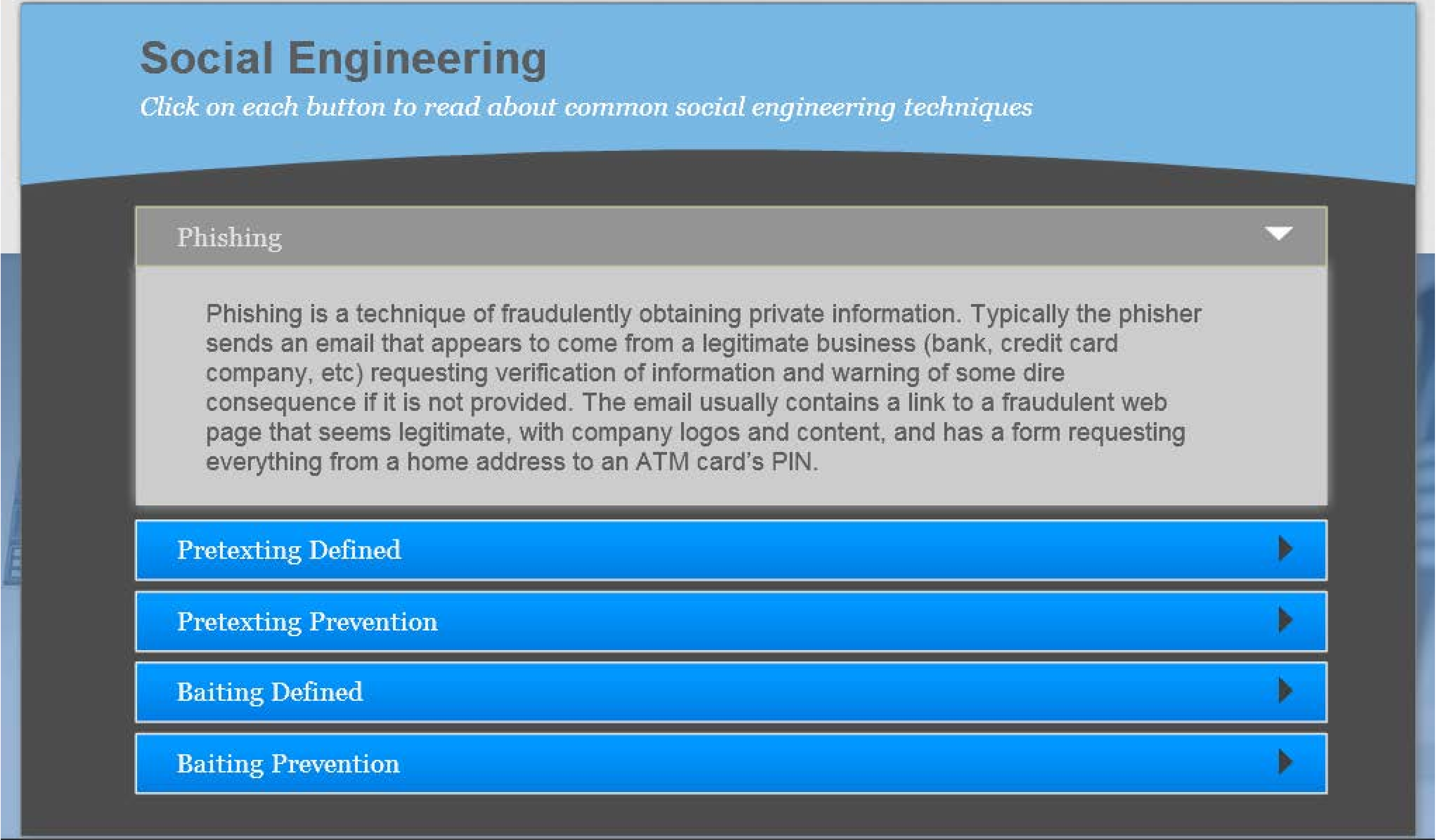
- Malicious email attachments
- Embedded malicious links
- Spam email

- Don't follow links within email, especially from an unfamiliar source
- Don't click on attachments from unknown senders
- Delete obvious spam without opening it

Cyber Crime - Social Engineering

Social engineering methods attackers use to gather the information needed for an attack include:

- Dumpster diving (going through a target’s trash)
- Persuasion
- Online communication
- Shoulder surfing
- Eavesdropping

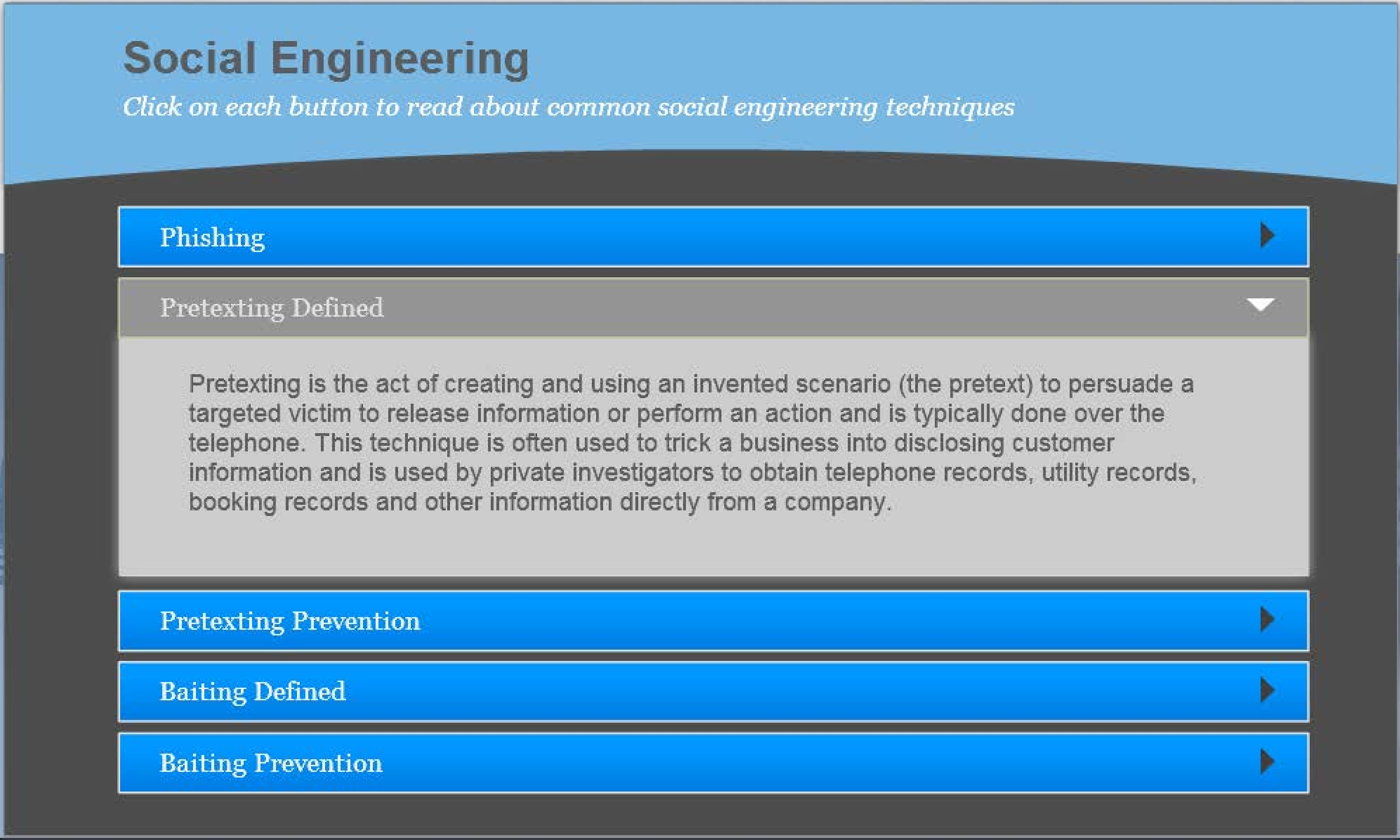


Social Engineering

Click on each button to read about common social engineering techniques

Phishing ▼

Phishing is a technique of fraudulently obtaining private information. Typically the phisher sends an email that appears to come from a legitimate business (bank, credit card company, etc) requesting verification of information and warning of some dire consequence if it is not provided. The email usually contains a link to a fraudulent web page that seems legitimate, with company logos and content, and has a form requesting everything from a home address to an ATM card's PIN.



Social Engineering

Click on each button to read about common social engineering techniques

Phishing ▸

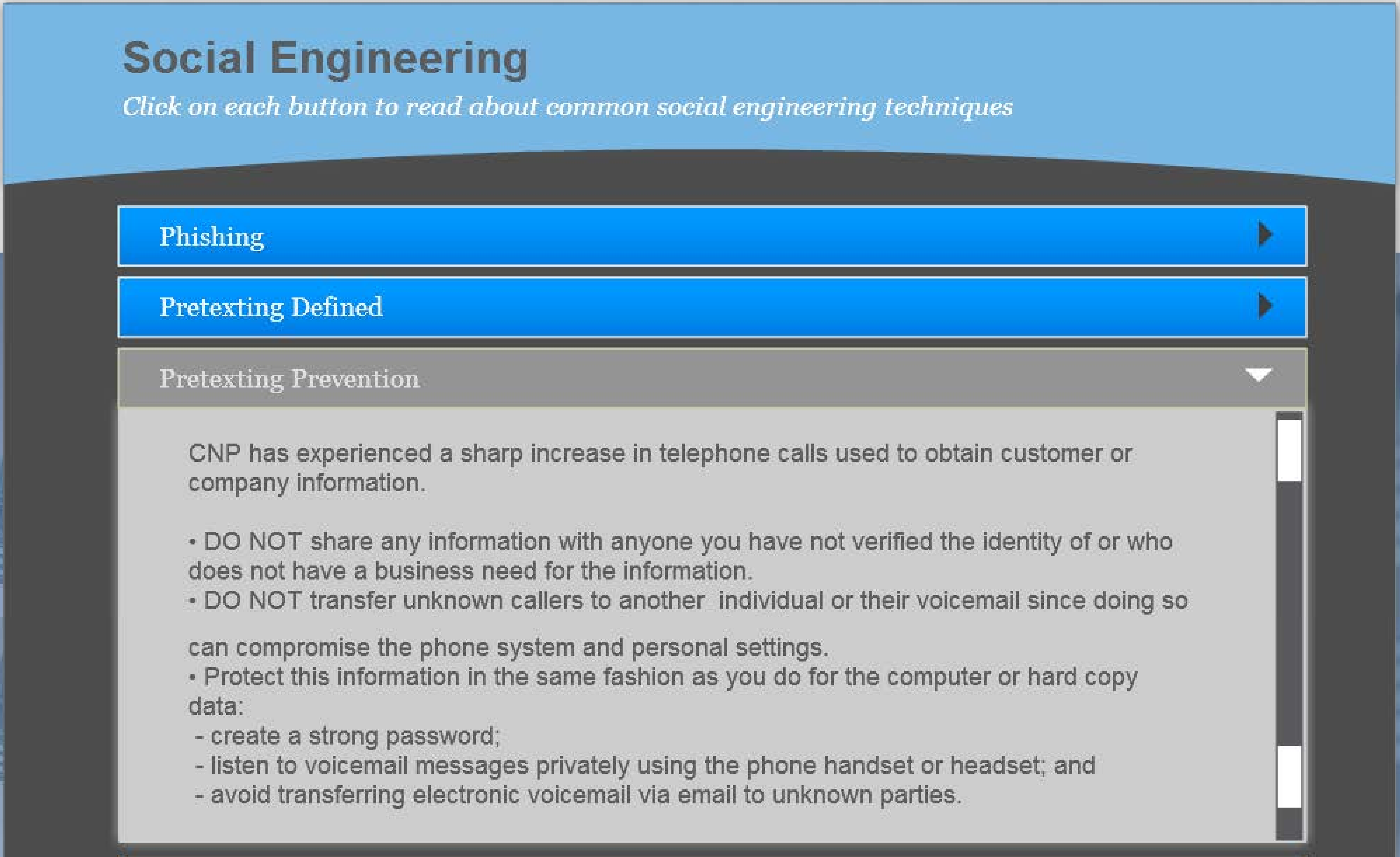
Pretexting Defined ▾

Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a targeted victim to release information or perform an action and is typically done over the telephone. This technique is often used to trick a business into disclosing customer information and is used by private investigators to obtain telephone records, utility records, booking records and other information directly from a company.

Pretexting Prevention ▸

Baiting Defined ▸

Baiting Prevention ▸



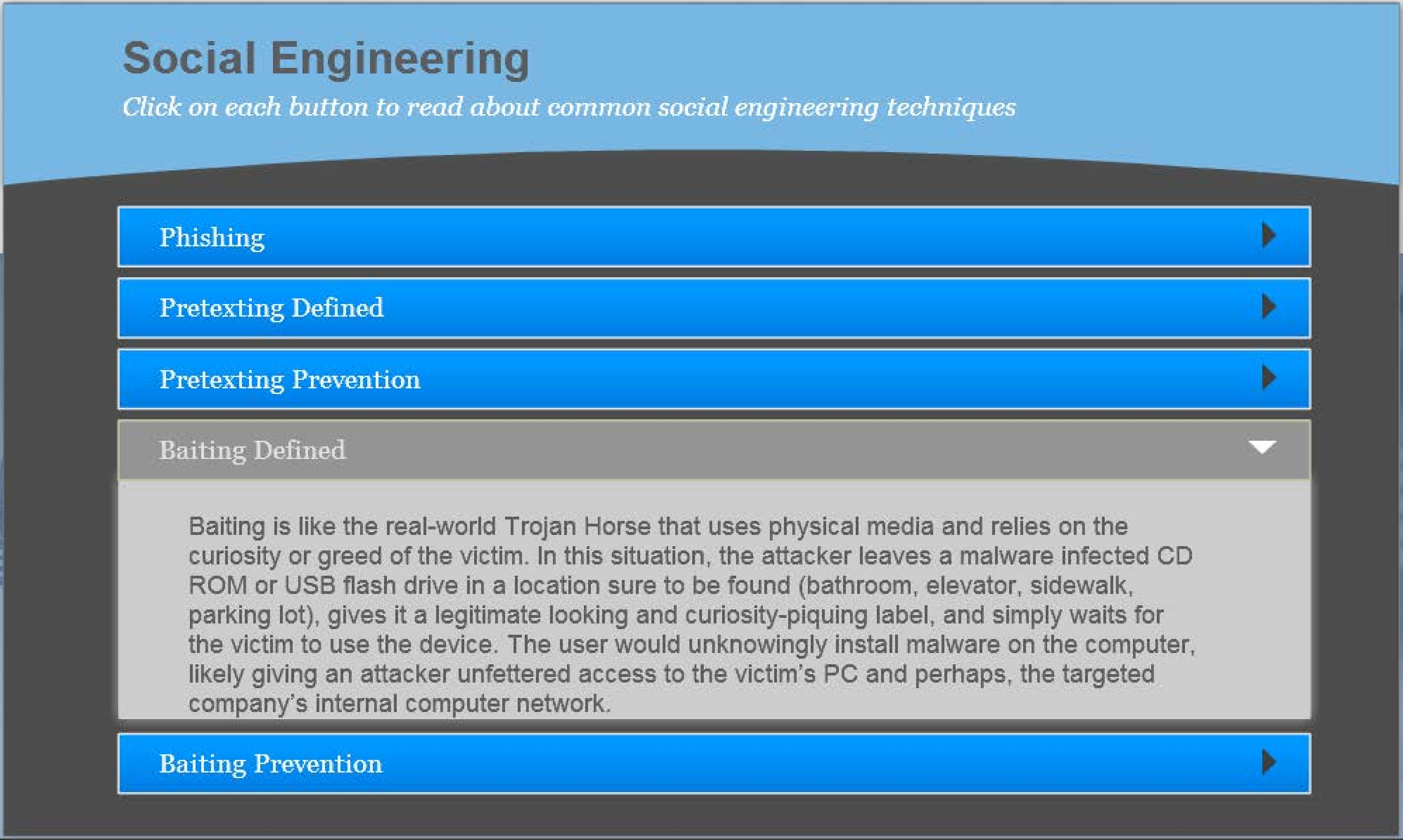
Social Engineering

Click on each button to read about common social engineering techniques

Pretexting Prevention

CNP has experienced a sharp increase in telephone calls used to obtain customer or company information.

- DO NOT share any information with anyone you have not verified the identity of or who does not have a business need for the information.
- DO NOT transfer unknown callers to another individual or their voicemail since doing so can compromise the phone system and personal settings.
- Protect this information in the same fashion as you do for the computer or hard copy data:
  - create a strong password;
  - listen to voicemail messages privately using the phone handset or headset; and
  - avoid transferring electronic voicemail via email to unknown parties.



Social Engineering

Click on each button to read about common social engineering techniques

Phishing ▶

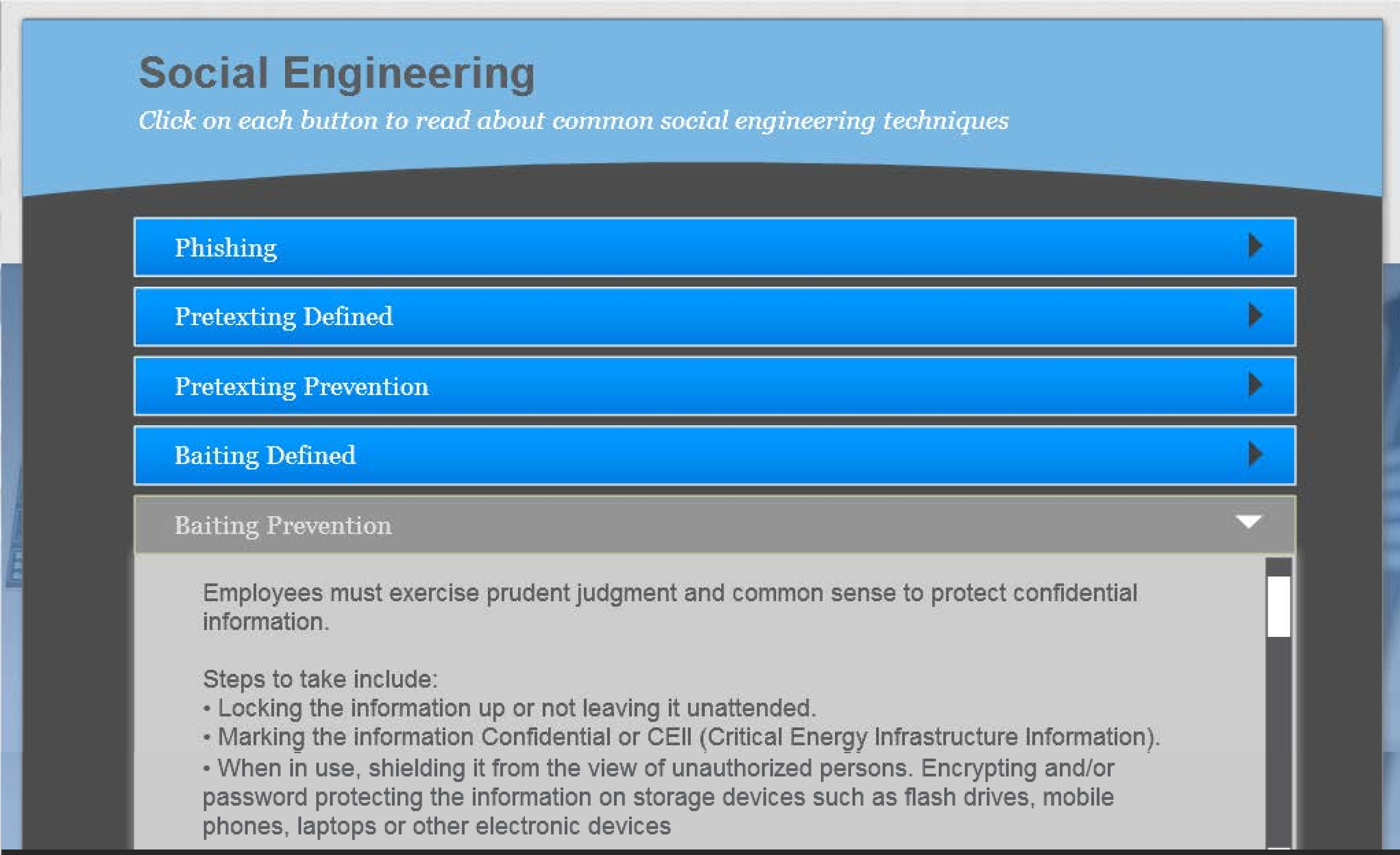
Pretexting Defined ▶

Pretexting Prevention ▶

Baiting Defined ▼

Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim. In this situation, the attacker leaves a malware infected CD ROM or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate looking and curiosity-piquing label, and simply waits for the victim to use the device. The user would unknowingly install malware on the computer, likely giving an attacker unfettered access to the victim's PC and perhaps, the targeted company's internal computer network.

Baiting Prevention ▶



Social Engineering

Click on each button to read about common social engineering techniques

Employees must exercise prudent judgment and common sense to protect confidential information.

Steps to take include:

- Locking the information up or not leaving it unattended.
- Marking the information Confidential or CEII (Critical Energy Infrastructure Information).
- When in use, shielding it from the view of unauthorized persons. Encrypting and/or password protecting the information on storage devices such as flash drives, mobile phones, laptops or other electronic devices

Cyber Security - Prevention

Proactive Steps for Prevention

Cyber Security - Prevention

Cybersecurity Risk Information Sharing Program (CRISP)

- voluntary program to share cybersecurity information between electric utilities and U.S. governmental agencies
- improve overall cyber security by sharing information of cyber threats and obtain any data analysis information provided by CRISP

Cyber Security - Prevention

Computer Use Policy

Cyber Security Measures

Critical Infrastructure

Computer Use Policy

Stealing and sharing copyrighted software, music, movies or downloading unauthorized software are not only violations of CNP's Use of Computer Resources policy, they are illegal! Employees can subject corporate networks to malware and virus threats through file sharing websites, downloading games, or using unapproved social media websites.

Cyber Security - Prevention

Computer Use Policy

Cyber Security Measures

Critical Infrastructure

Cyber Security Measures

Cyber and Supervisory Control & Data Acquisition (SCADA) system security measures are vital to the protection of important company information and control systems. Measures taken to protect these information systems include:

- On-access virus scanning and weekly vulnerability scanning
- Company Internet and SCADA firewalls
- Password protection and frequent password changing for all computers
- Utilization of secure (encrypted) data transport mechanisms

Cyber Security - Prevention

Computer Use Policy

Cyber Security Measures

Critical Infrastructure

Critical Infrastructure

CNP secures critical infrastructure control systems by:

- special access requirements to SCADA control rooms
- separate computer systems and networks for the SCADA system
- employees and contractors keeping information about critical assets and systems confidential

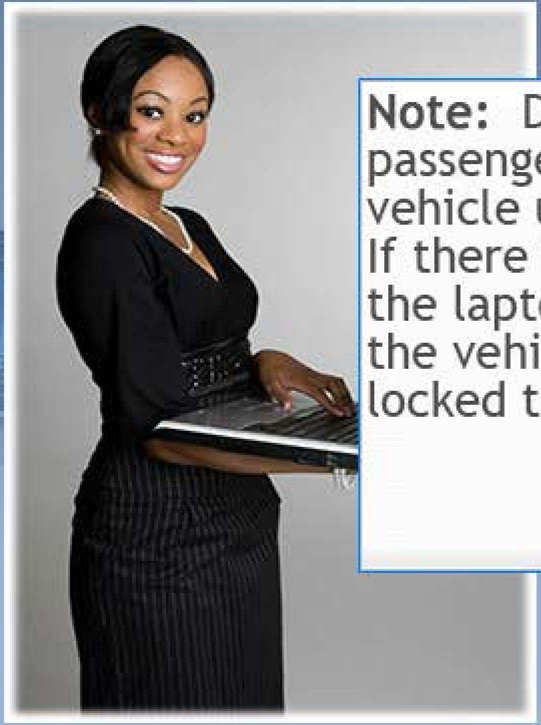
Cyber Security - Prevention

Laptops

- Lock the Screen (Control ALT Delete)
- Do not leave laptops unattended
- Never leave a company laptop unattended and visible in a vehicle

Cyber Security - Prevention

Laptops



Note: Do not leave a company laptop computer in the passenger compartment of a company or personal vehicle unless it is secured in a locked docking station. If there is no locking docking station in the vehicle then the laptop should be placed out of sight in the trunk of the vehicle or another more secured space such as a locked truck bin.

Continue

)elete)

d

icle

Cyber Security - Prevention

Passwords

- Do not leave written passwords in the open or accessible to others
- Choose complex passwords containing symbols, numbers and letters
- Change your passwords regularly
- Never use the same password for CNP systems you use for personal systems
- Do not share your password
- Use encryption and password protection for valuable files

Physical Security

Physical Security - Introduction

What is Physical Security?

Physical Security refers to measures that help protect facilities, personnel, assets or information stored on physical media.

The formula for a successful security program combines physical security measures and operational practices with an informed, security-aware, and alert workforce.

Physical Security - Best Practices

Click on a topic to learn more

- Be Alert
- Company Vehicles
- Mobile Devices
- Work Access
- Personal Property
- ID Badge
- Keys
- Suspicious Activity

Physical Security - Best Practices

Be Alert!

- Always park in well-lit areas
- Keep access doors and gates secure
- Do not accept suspicious packages or deliveries and DO NOT OPEN THEM
- Be aware of suspicious persons or suspicious behavior

Physical Security - Best Practices

Company Vehicles

- Keep locked when the vehicle is unattended
- Do not leave keys in unattended vehicles
- When so equipped, set vehicle alarms and carry portable alarms
- Secure all equipment, tools, and high value materials in a manner to prevent theft

Physical Security - Best Practices

Mobile Devices

- Mobile devices should never be left in a vacant car.
- Never leave unattended in public places like conference rooms, airports, restrooms, public transport, etc.
- Should be kept with the user the whole time, or stored in a facility with no public access – e.g., a room or an office that is locked when no one is present.

Physical Security - Best Practices

Work Access

- Keep access doors to your work area locked to prevent unauthorized access
- Do not allow entry or tailgating to persons you do not know into your work areas
- Do not prop doors open or circumvent locks

Physical Security - Best Practices

Work Access

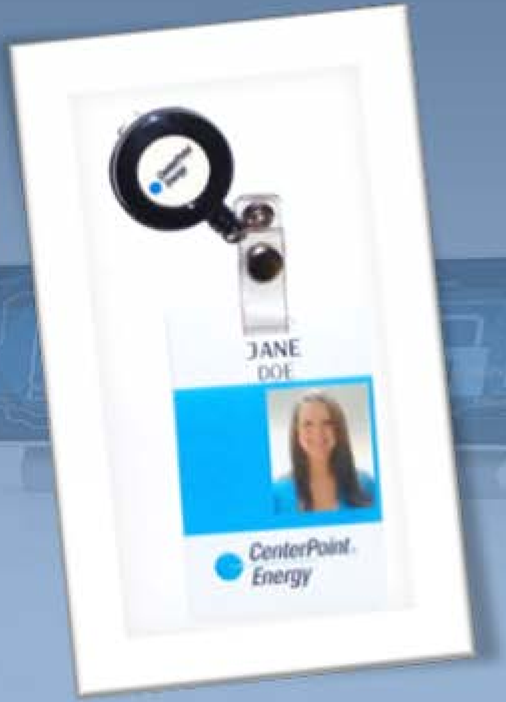
- Escort your visitors when in secured areas
- Shut, secure and arm alarm systems for all doors and gates when leaving a facility unoccupied
- Challenge or report strangers in the workplace

Physical Security - Best Practices

Personal Property

- Lock your personal vehicle
- Don't leave valuables visible in your vehicle
- Do not leave personal items accessible that you value when your work area is unoccupied

Physical Security - Best Practices



ID Badge

- It is issued solely for your specific use
- It cannot be transferred to another person
- You should keep it protected from unauthorized use
- It should be surrendered to management upon termination

Physical Security - Best Practices

ID Badge

- It should be worn visibly while on property
- You should report lost or stolen badges immediately to your supervisor and Corporate Security

Physical Security - Best Practices

Keys

- Issued solely for your specific use
- Cannot be transferred to another person,
- Should be kept protected from unauthorized use
- Remains the property of the Company, and
- Must be returned when no longer required.

Physical Security - Best Practices

Recognizing Suspicious Activity

A suspicious activity is defined as when a person’s conduct or action does not fit the normal activity, or seems out-of-place for the time or location.

Report suspicious activity

- Immediately call 911 to report illegal activity to law enforcement.
- Report suspicious activity and persons to management or Corporate Security at the 24/7 Security Operations Center, 713-207-5500.

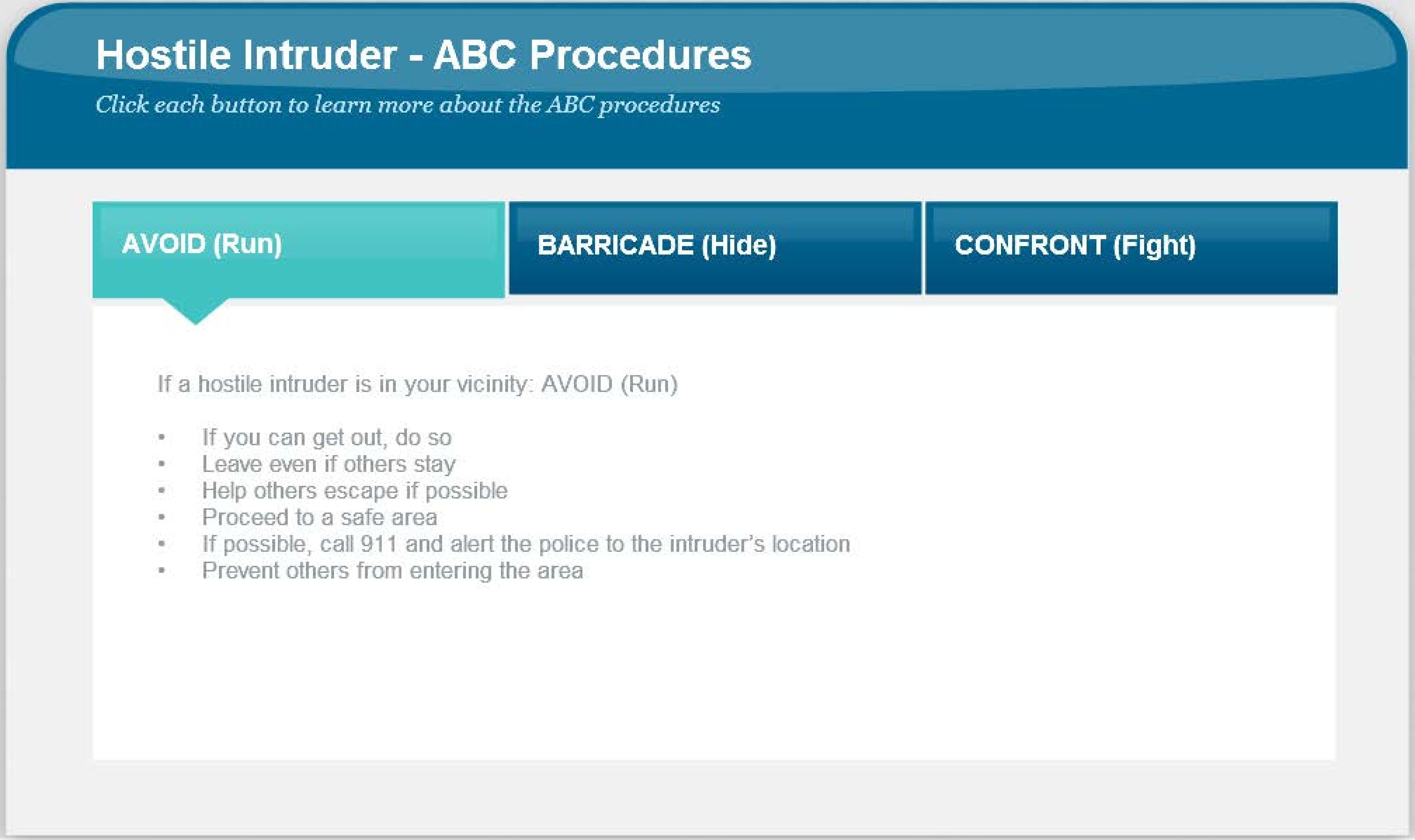
Physical Security - Hostile Intruder

Know:

- Where are the paths of escape?
- Where could I hide?
- Do I know what to do if an event occurs?

Determine your course of action with the ABC procedures:

- Avoid
- Barricade
- Confront

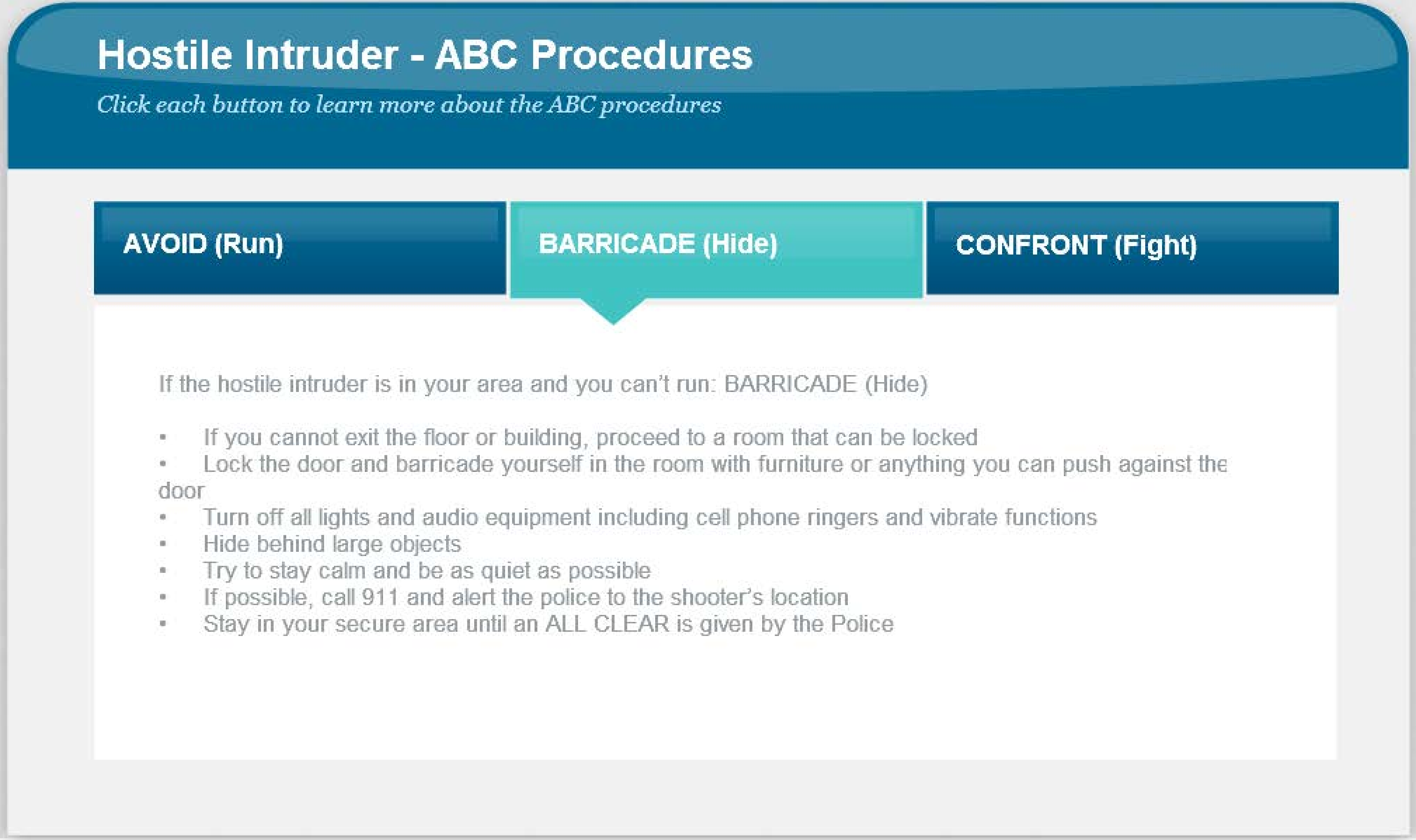


Hostile Intruder - ABC Procedures

Click each button to learn more about the ABC procedures

If a hostile intruder is in your vicinity: AVOID (Run)

- If you can get out, do so
- Leave even if others stay
- Help others escape if possible
- Proceed to a safe area
- If possible, call 911 and alert the police to the intruder’s location
- Prevent others from entering the area

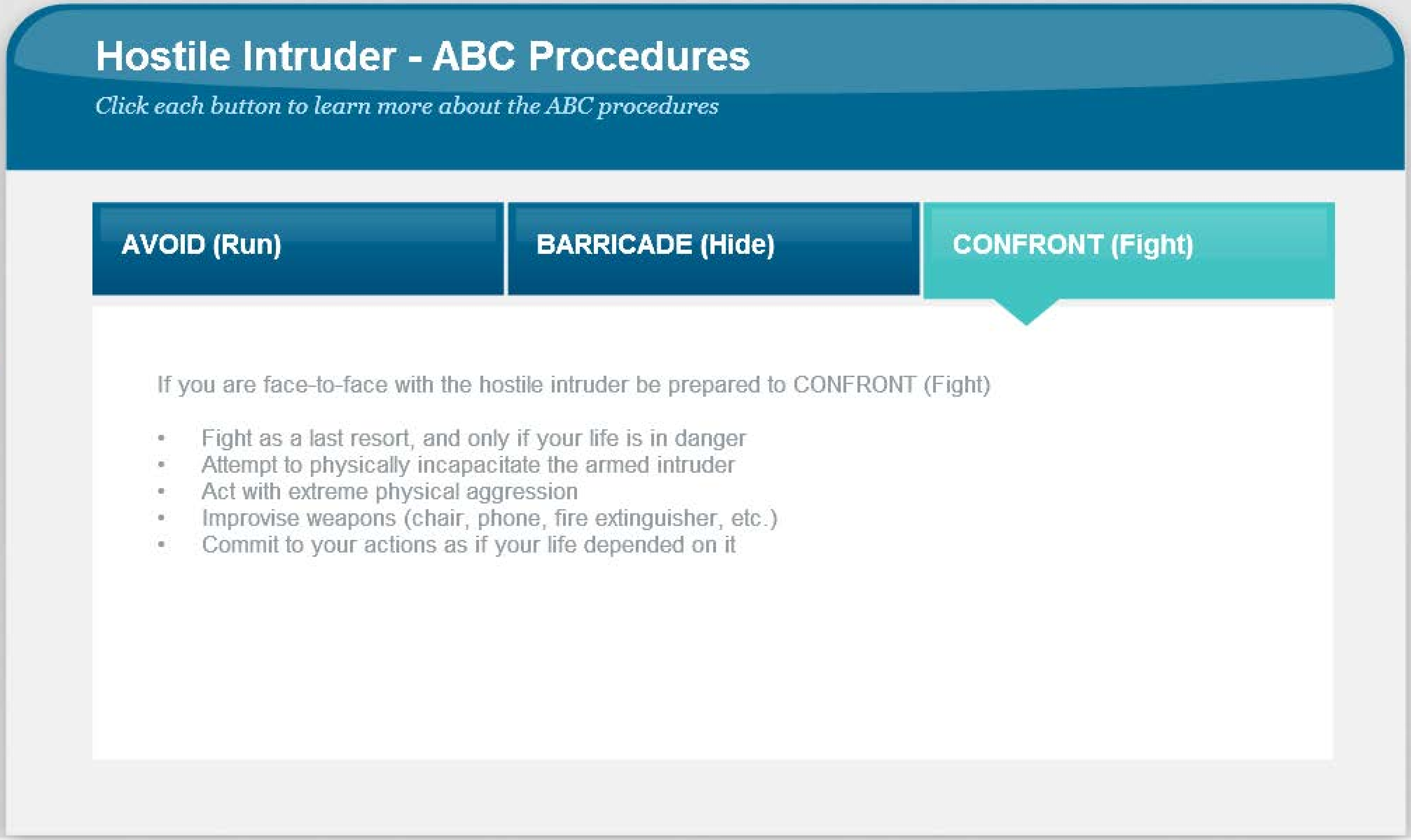


Hostile Intruder - ABC Procedures

Click each button to learn more about the ABC procedures

If the hostile intruder is in your area and you can't run: BARRICADE (Hide)

- If you cannot exit the floor or building, proceed to a room that can be locked
- Lock the door and barricade yourself in the room with furniture or anything you can push against the door
- Turn off all lights and audio equipment including cell phone ringers and vibrate functions
- Hide behind large objects
- Try to stay calm and be as quiet as possible
- If possible, call 911 and alert the police to the shooter's location
- Stay in your secure area until an ALL CLEAR is given by the Police



Hostile Intruder - ABC Procedures

Click each button to learn more about the ABC procedures

If you are face-to-face with the hostile intruder be prepared to CONFRONT (Fight)

- Fight as a last resort, and only if your life is in danger
- Attempt to physically incapacitate the armed intruder
- Act with extreme physical aggression
- Improvise weapons (chair, phone, fire extinguisher, etc.)
- Commit to your actions as if your life depended on it

Physical Security - Hostile Intruder

The police will not know who is a threat and who is not a threat, keep your hands in the air.

Physical Security - Hostile Intruder

Click the button
to watch the video

Physical Security

- Report any threatening communications
- Report suspicious activity on or around company facilities
- Report persons photographing or surveilling company facilities or infrastructure
- Report suspicious packages or mail

Congratulations!

You have successfully completed
the Security Awareness course.

Go to the next page of this PDF
to print out the completion certificate.

Certificate of Completion

Security Awareness Training

I certify that I have completed the *Security Awareness 2016-17* training course and that I will comply with the requirements.

Date: ____

Signature: ____

Printed Name: ____

Company (Vendor) Name: _____________________________________

Print and complete two (2) copies of this certification. Keep one for your records. Forward the other copy to your management or appropriate representative within your company.

Please note that you are required to complete this training within 30 days of the date you begin providing contract services for CenterPoint Energy and repeat as mandated thereafter. You and/or your company may be required to produce this certification upon request as evidence of your compliance with this requirement.