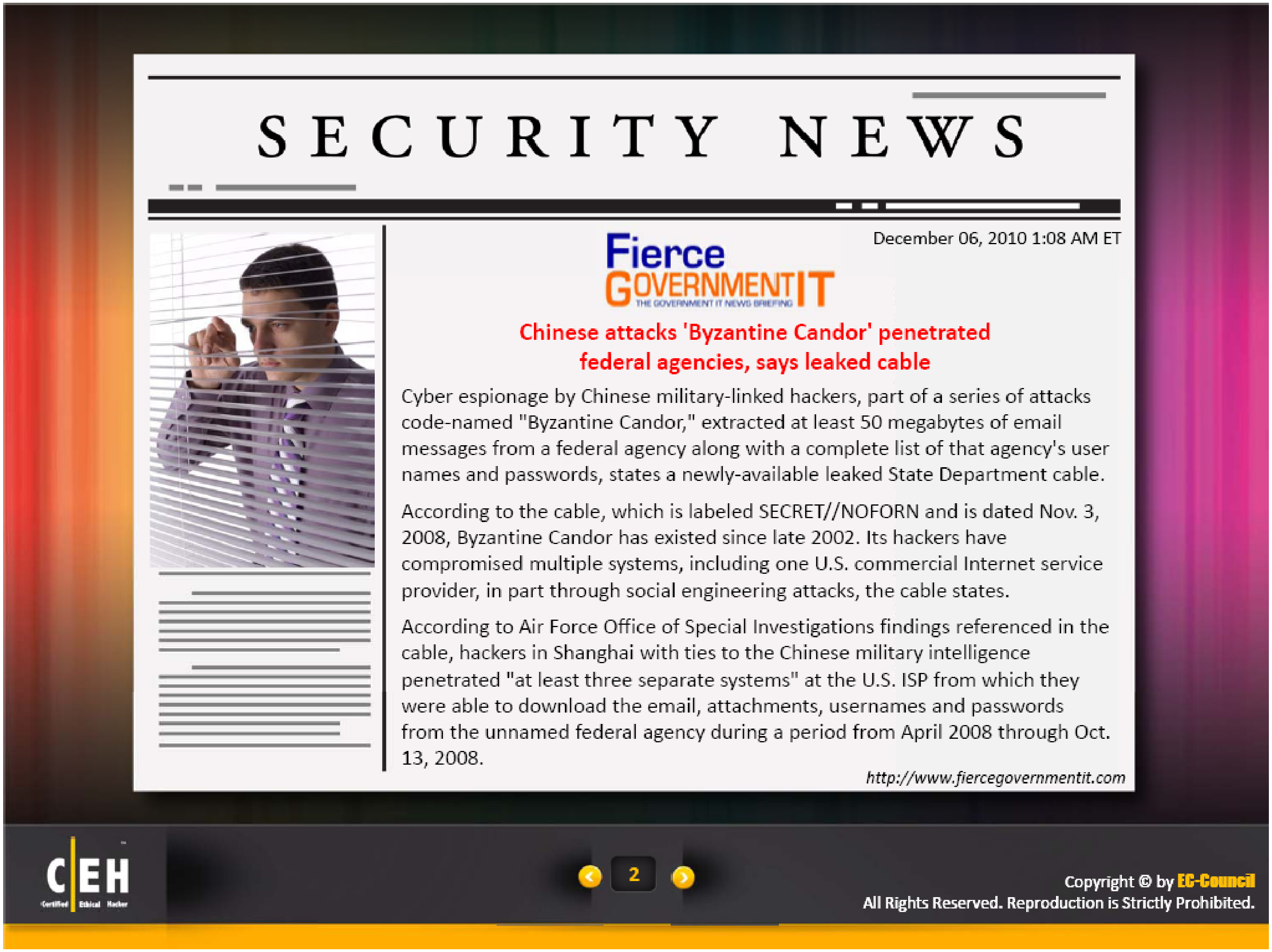
Social Engineering

Module 9

Engineered by Hackers. Presented by Professionals.

C|EH™

Certified Ethical Hacker



SECURITY NEWS

December 06, 2010 1:08 AM ET

FierceGovernmentIT
THE GOVERNMENT IT NEWS BRIEFING

Chinese attacks 'Byzantine Candor' penetrated federal agencies, says leaked cable

Cyber espionage by Chinese military-linked hackers, part of a series of attacks code-named "Byzantine Candor," extracted at least 50 megabytes of email messages from a federal agency along with a complete list of that agency's user names and passwords, states a newly-available leaked State Department cable.

According to the cable, which is labeled SECRET//NOFORN and is dated Nov. 3, 2008, Byzantine Candor has existed since late 2002. Its hackers have compromised multiple systems, including one U.S. commercial Internet service provider, in part through social engineering attacks, the cable states.

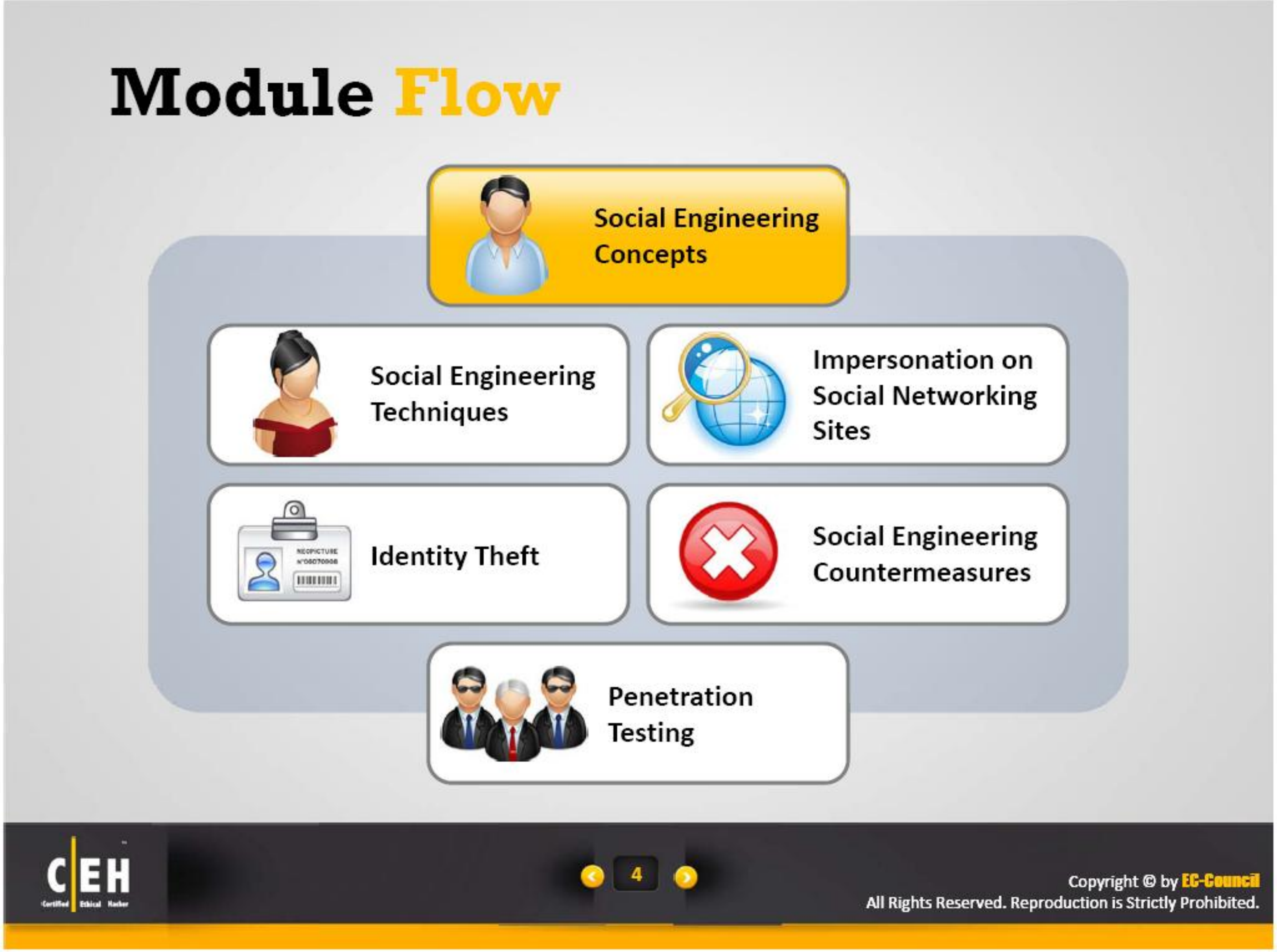
According to Air Force Office of Special Investigations findings referenced in the cable, hackers in Shanghai with ties to the Chinese military intelligence penetrated "at least three separate systems" at the U.S. ISP from which they were able to download the email, attachments, usernames and passwords from the unnamed federal agency during a period from April 2008 through Oct. 13, 2008.

http://www.fiercegovernmentit.com

Module Objectives

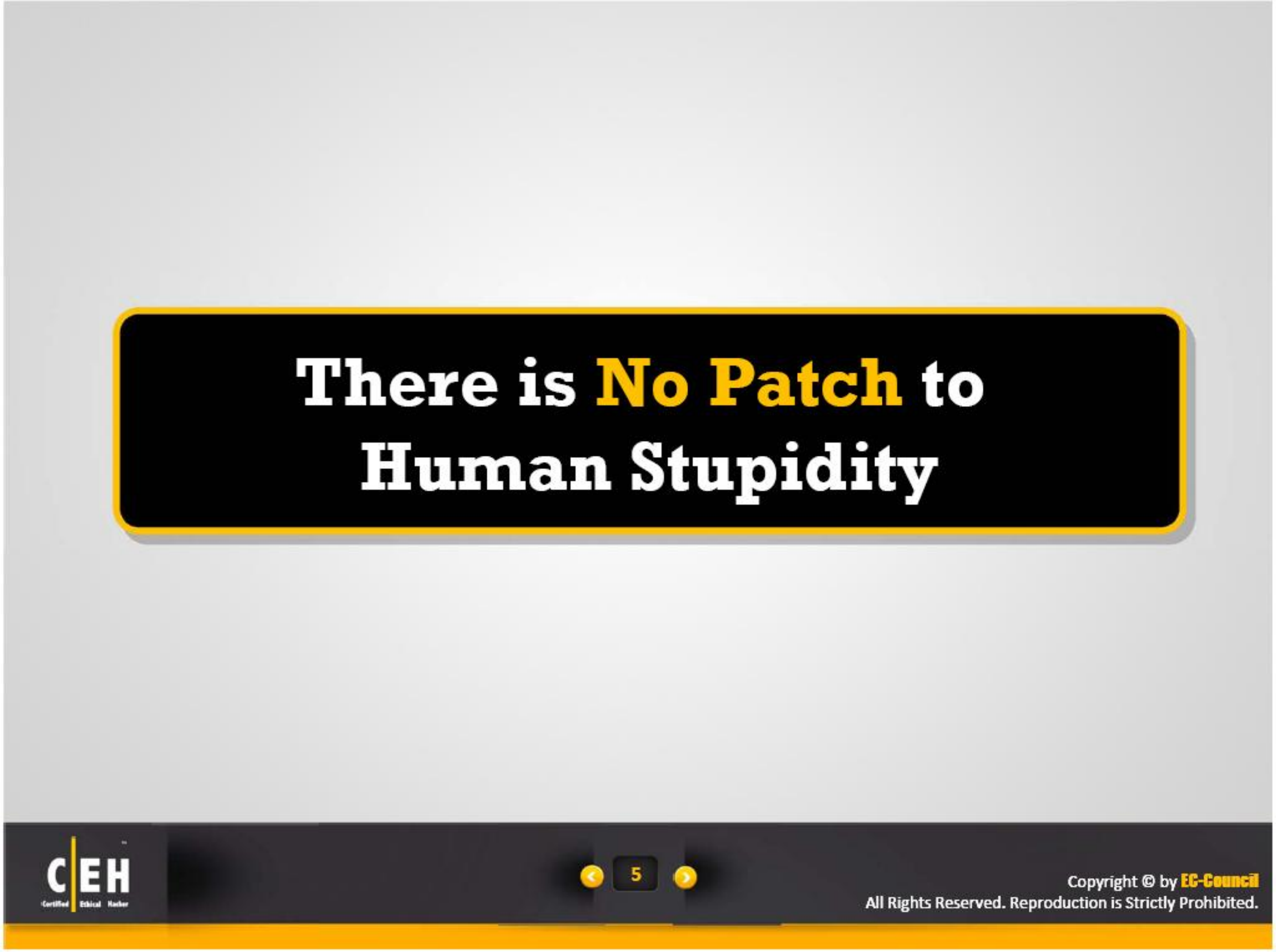
- What is Social Engineering?
- Why is Social Engineering Effective?
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Types of Social Engineering
- Common Intrusion Tactics and Strategies for Prevention

- Social Engineering Through Impersonation on Social Networking Sites
- Risks of Social Networking to Corporate Networks
- Identify Theft
- How to Steal Identity?
- Social Engineering Countermeasures
- Social Engineering Pen Testing

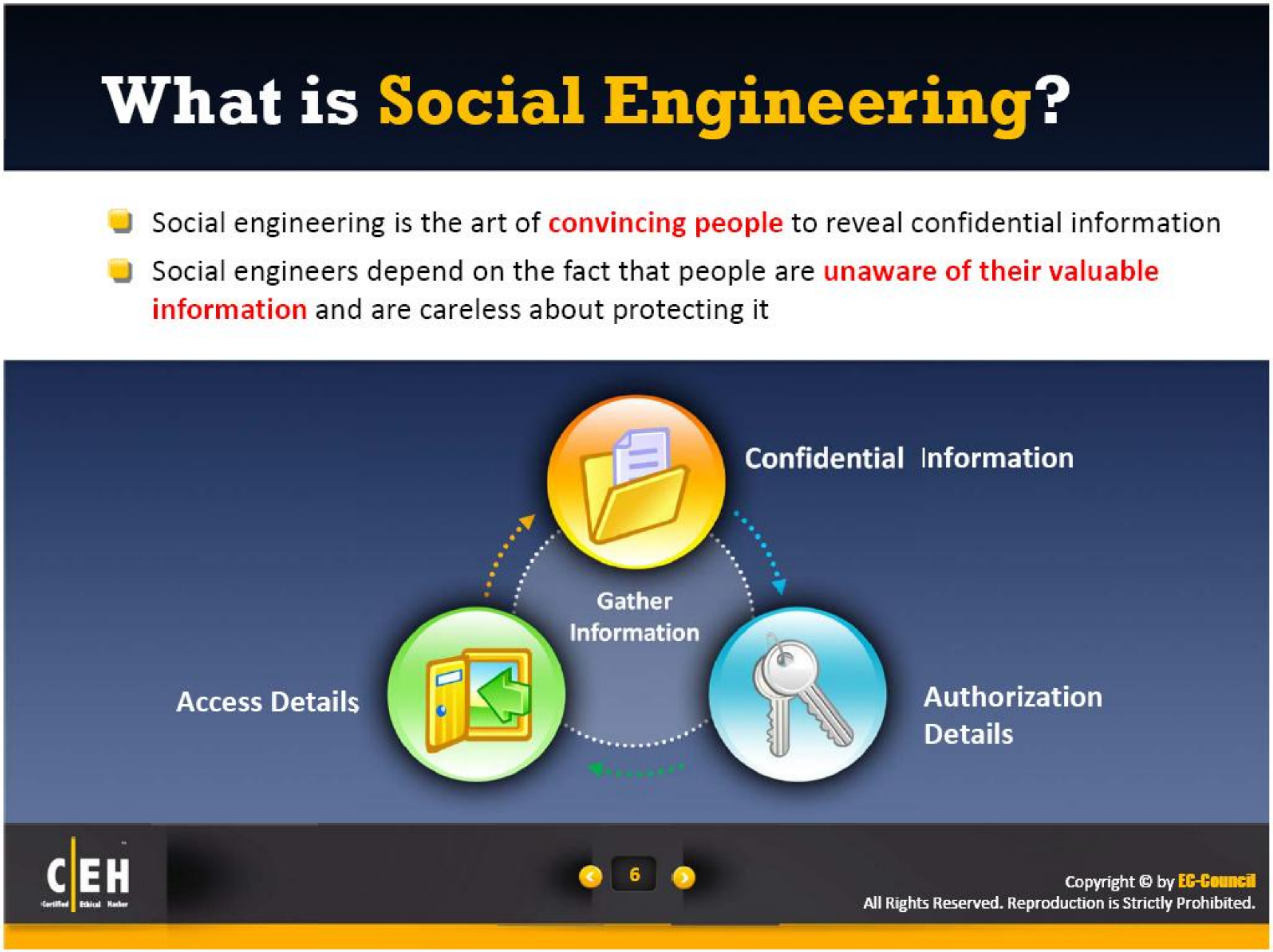


Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing

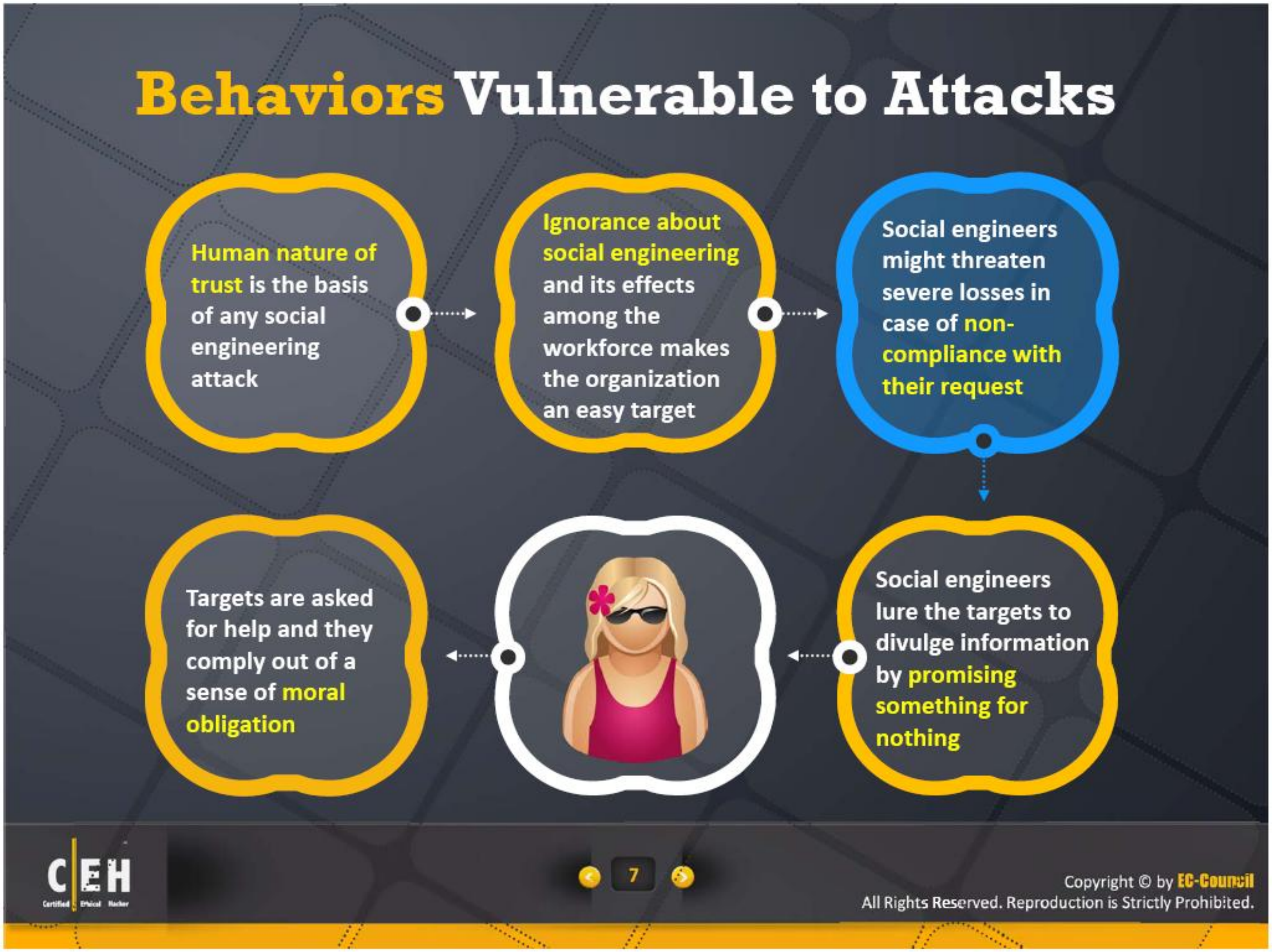


There is No Patch to Human Stupidity



What is Social Engineering?

- Social engineering is the art of **convincing people** to reveal confidential information
- Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it



Behaviors Vulnerable to Attacks

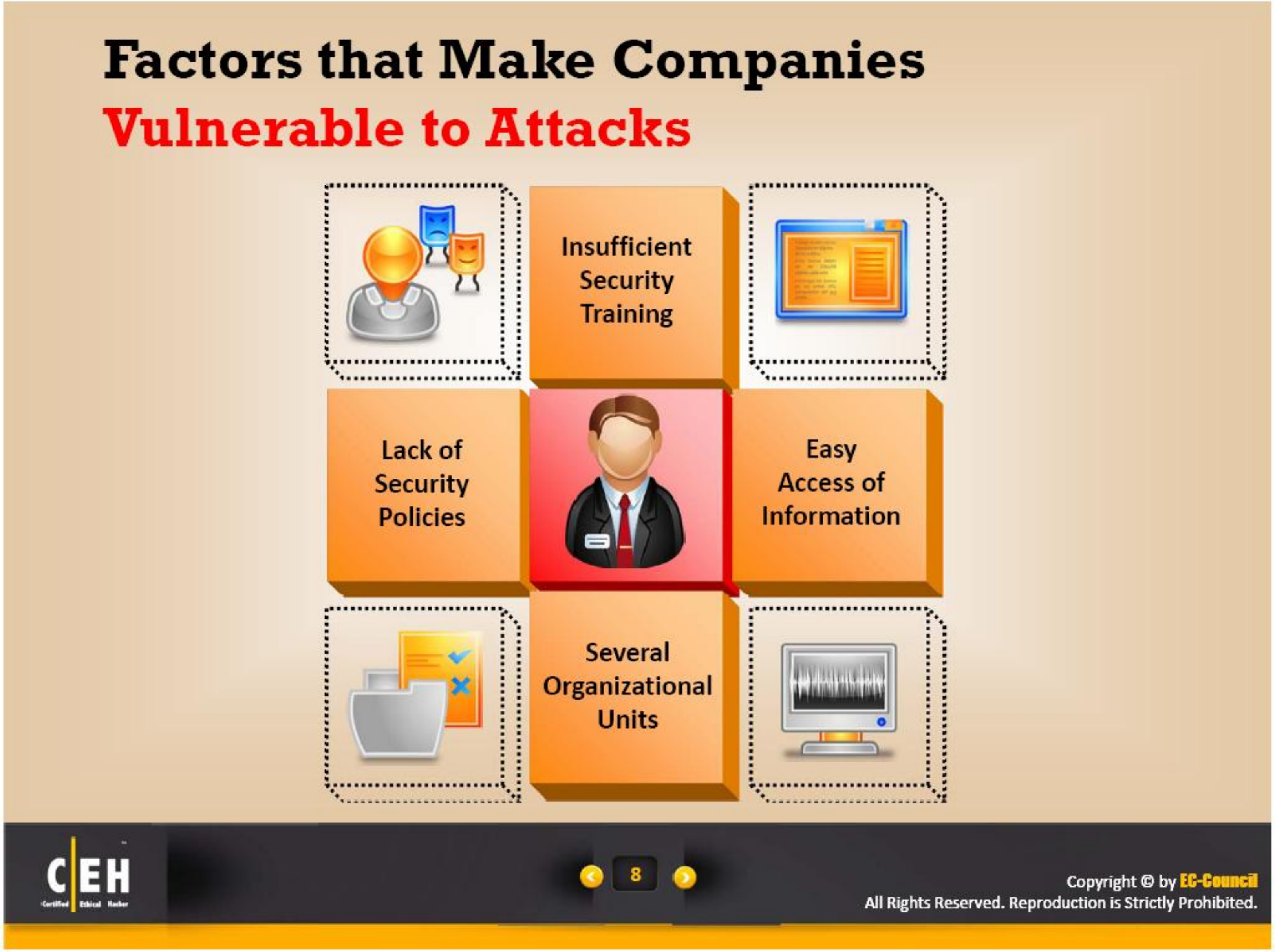
Human nature of trust is the basis of any social engineering attack

Ignorance about social engineering and its effects among the workforce makes the organization an easy target

Social engineers might threaten severe losses in case of non-compliance with their request

Social engineers lure the targets to divulge information by promising something for nothing

Targets are asked for help and they comply out of a sense of moral obligation



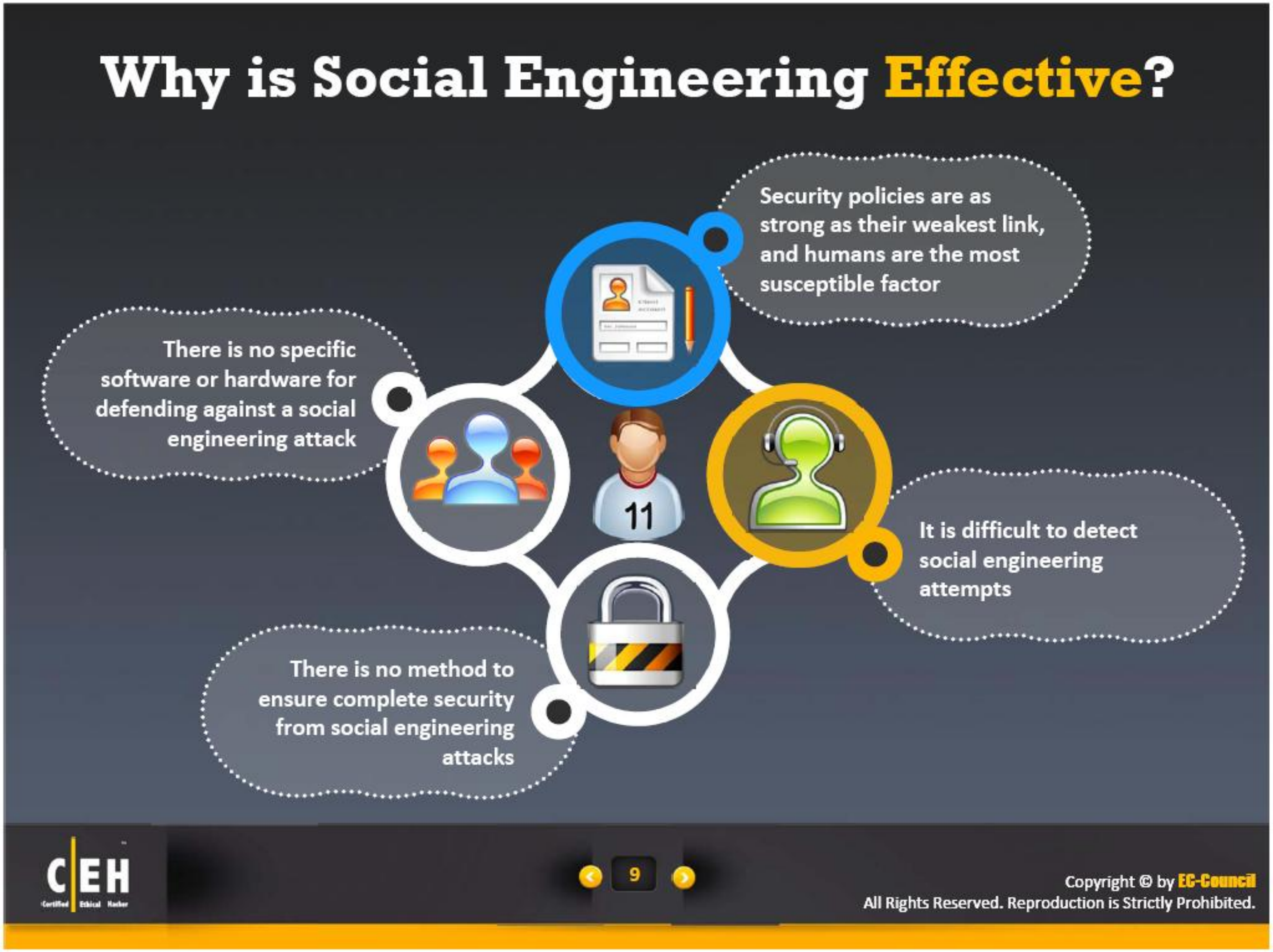
Factors that Make Companies Vulnerable to Attacks

Insufficient Security Training

Lack of Security Policies

Easy Access of Information

Several Organizational Units



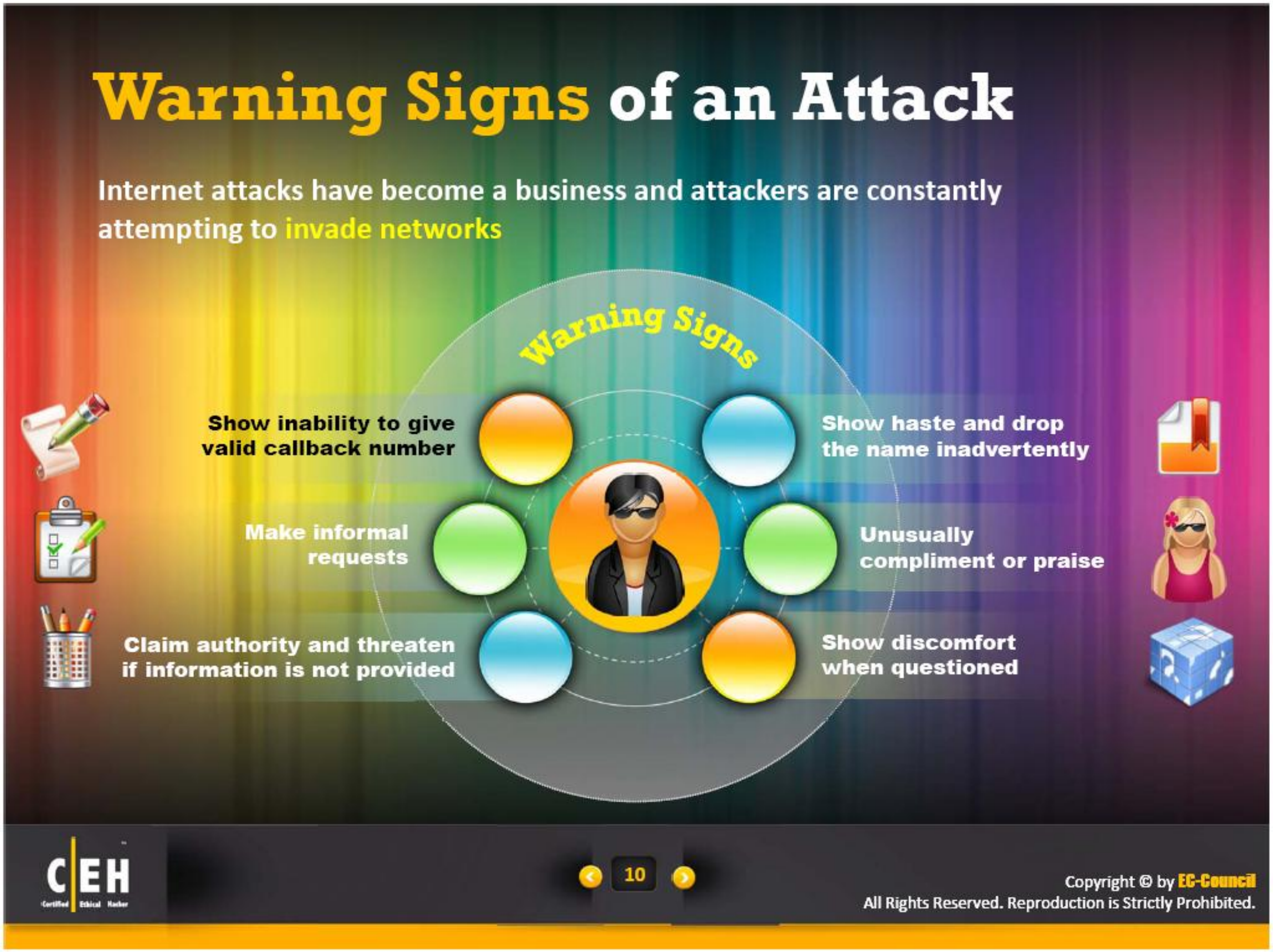
Why is Social Engineering Effective?

Security policies are as strong as their weakest link, and humans are the most susceptible factor

There is no specific software or hardware for defending against a social engineering attack

It is difficult to detect social engineering attempts

There is no method to ensure complete security from social engineering attacks

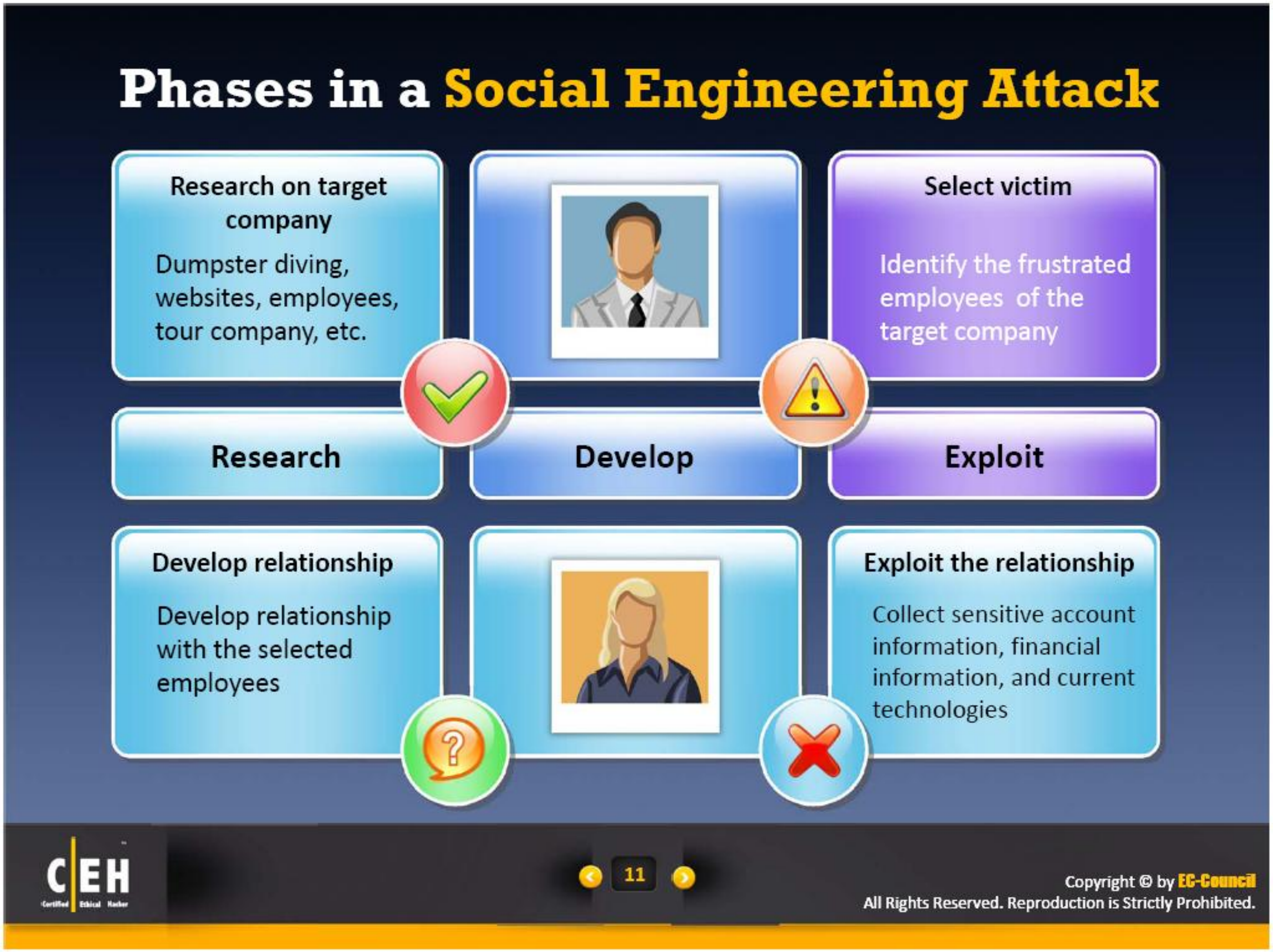


Warning Signs of an Attack

Internet attacks have become a business and attackers are constantly attempting to invade networks

Warning Signs

- Show inability to give valid callback number
- Make informal requests
- Claim authority and threaten if information is not provided
- Show haste and drop the name inadvertently
- Unusually compliment or praise
- Show discomfort when questioned



Phases in a Social Engineering Attack

Research on target company

Dumpster diving, websites, employees, tour company, etc.

Select victim

Identify the frustrated employees of the target company

Research

Develop

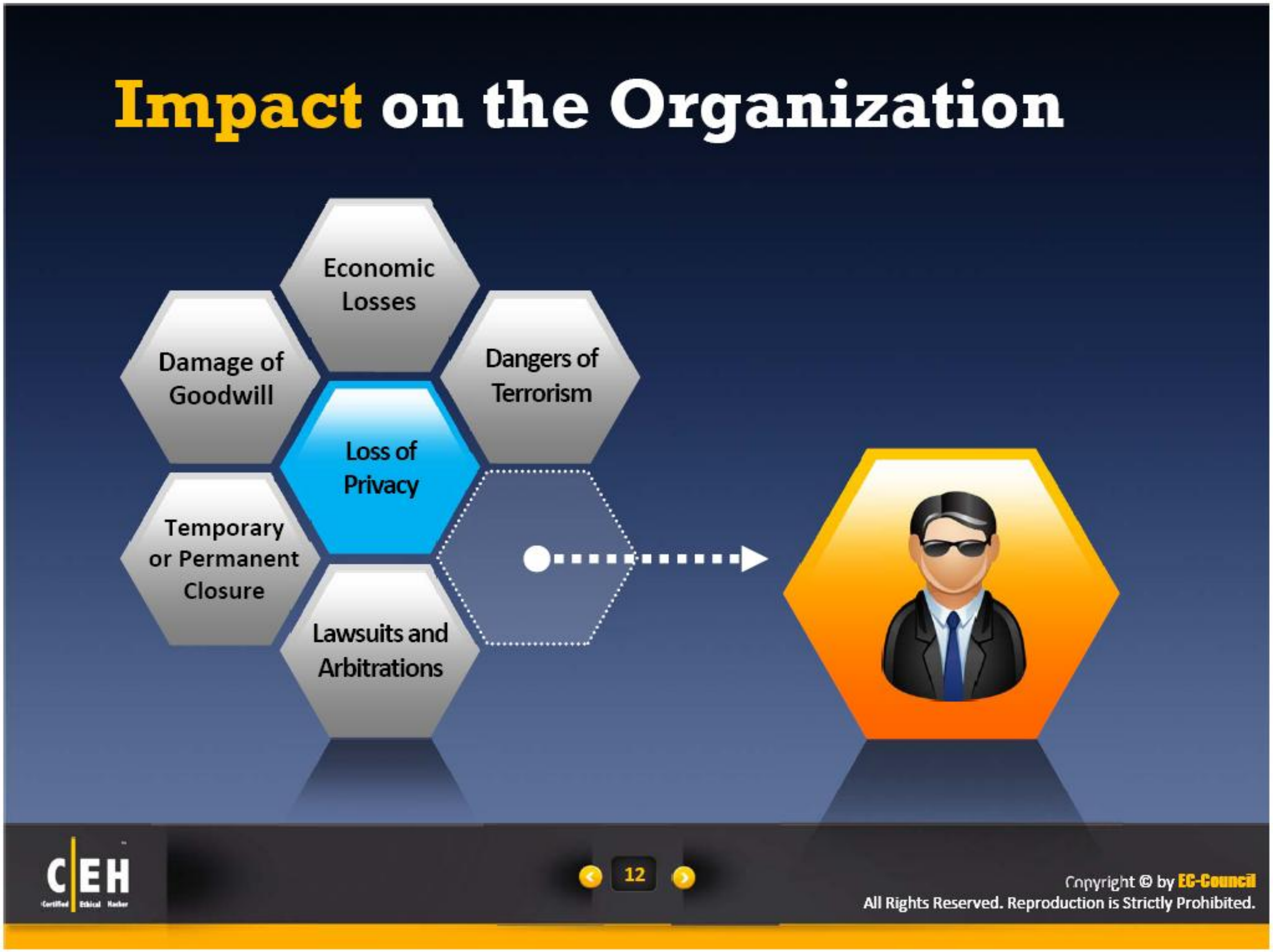
Exploit

Develop relationship

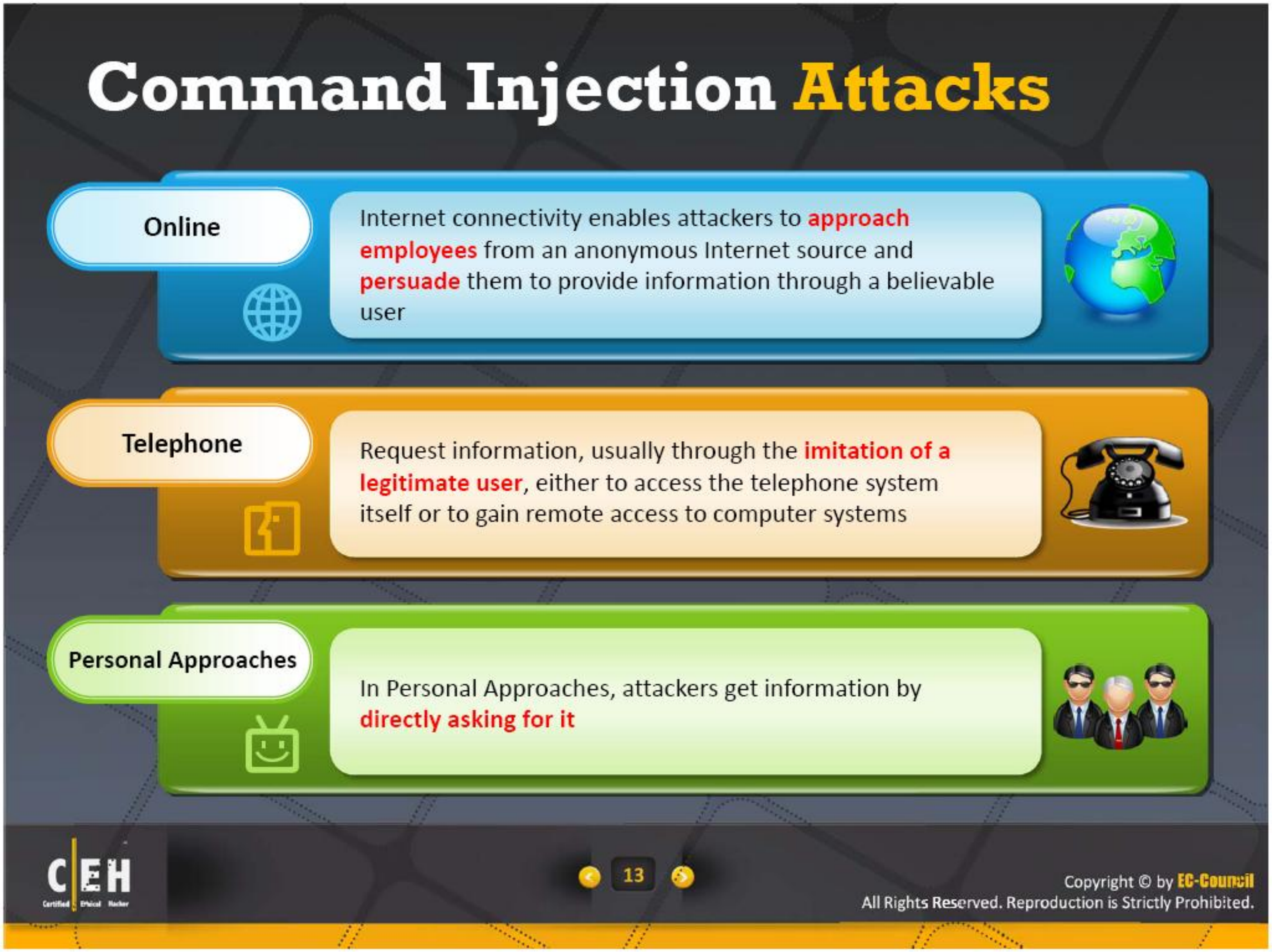
Develop relationship with the selected employees

Exploit the relationship

Collect sensitive account information, financial information, and current technologies



Impact on the Organization



Command Injection Attacks

Online

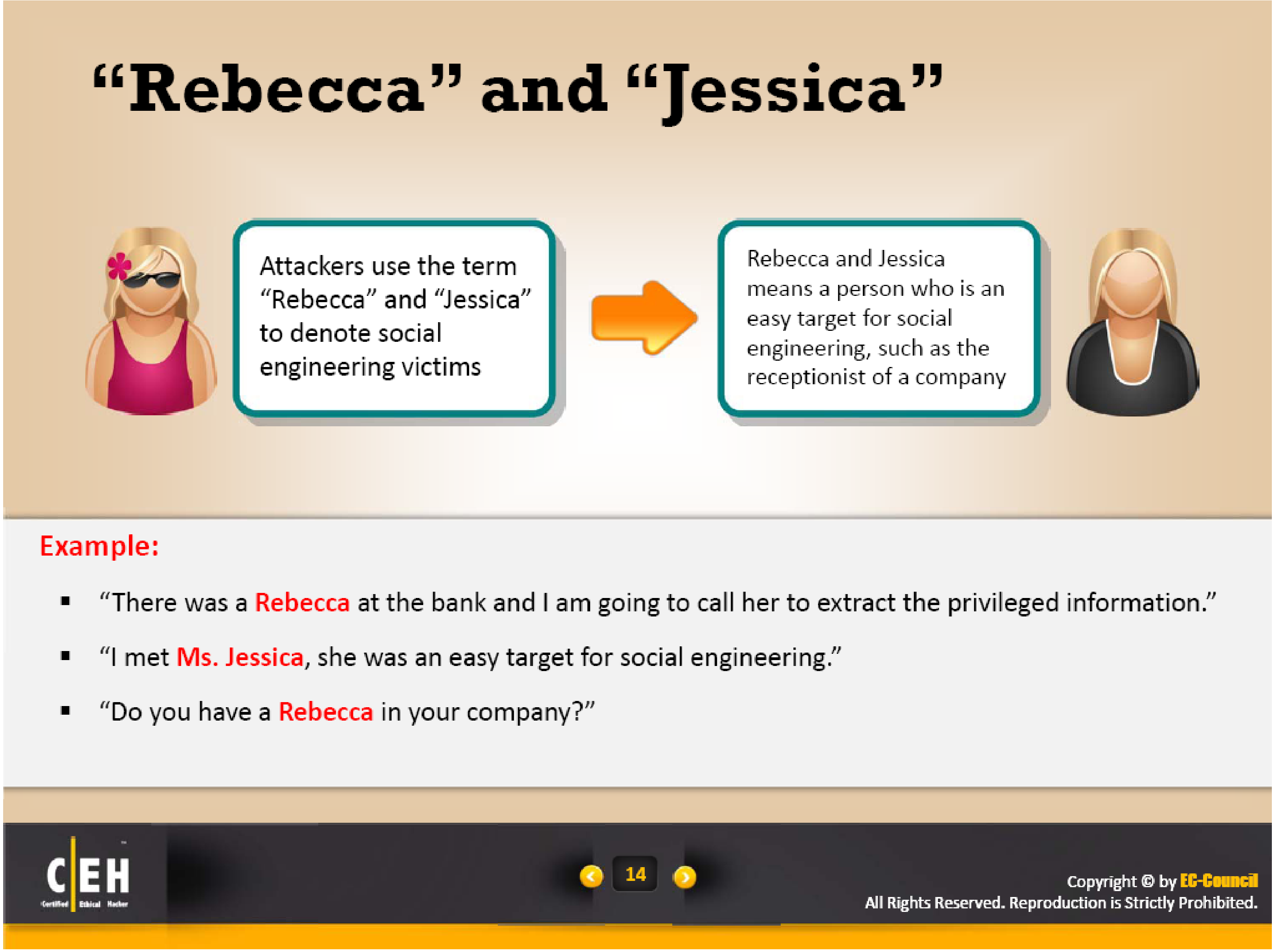
Internet connectivity enables attackers to **approach employees** from an anonymous Internet source and **persuade** them to provide information through a believable user

Telephone

Request information, usually through the **imitation of a legitimate user**, either to access the telephone system itself or to gain remote access to computer systems

Personal Approaches

In Personal Approaches, attackers get information by **directly asking for it**



“Rebecca” and “Jessica”

Attackers use the term “Rebecca” and “Jessica” to denote social engineering victims

Rebecca and Jessica means a person who is an easy target for social engineering, such as the receptionist of a company

Example:

- “There was a Rebecca at the bank and I am going to call her to extract the privileged information.”
- “I met Ms. Jessica, she was an easy target for social engineering.”
- “Do you have a Rebecca in your company?”

Common Targets of Social Engineering

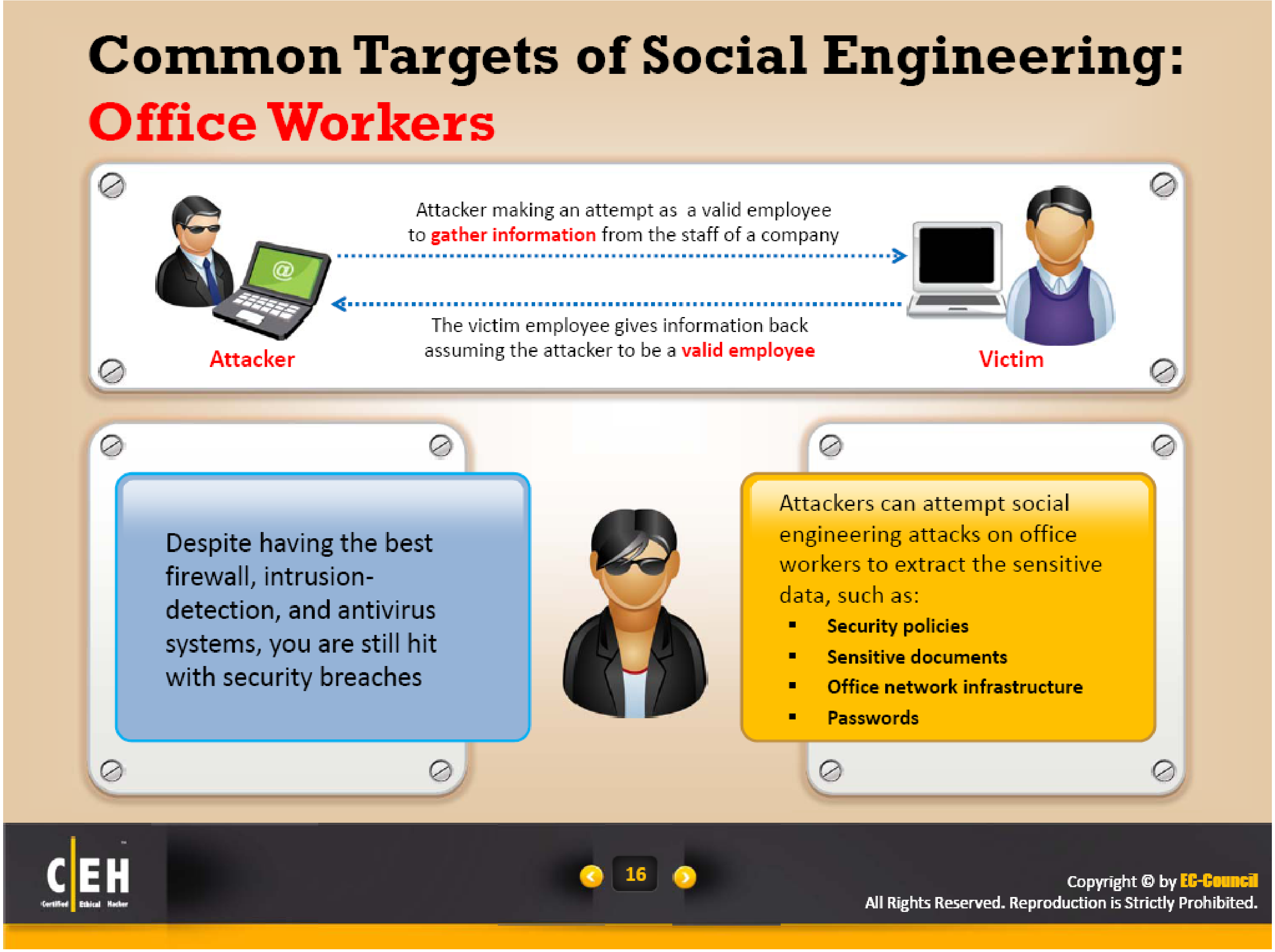
Receptionists & Help Desk Personnel

Users and Clients

Technical Support Executives

Vendors of the Target Organization

System Administrators



Common Targets of Social Engineering: Office Workers

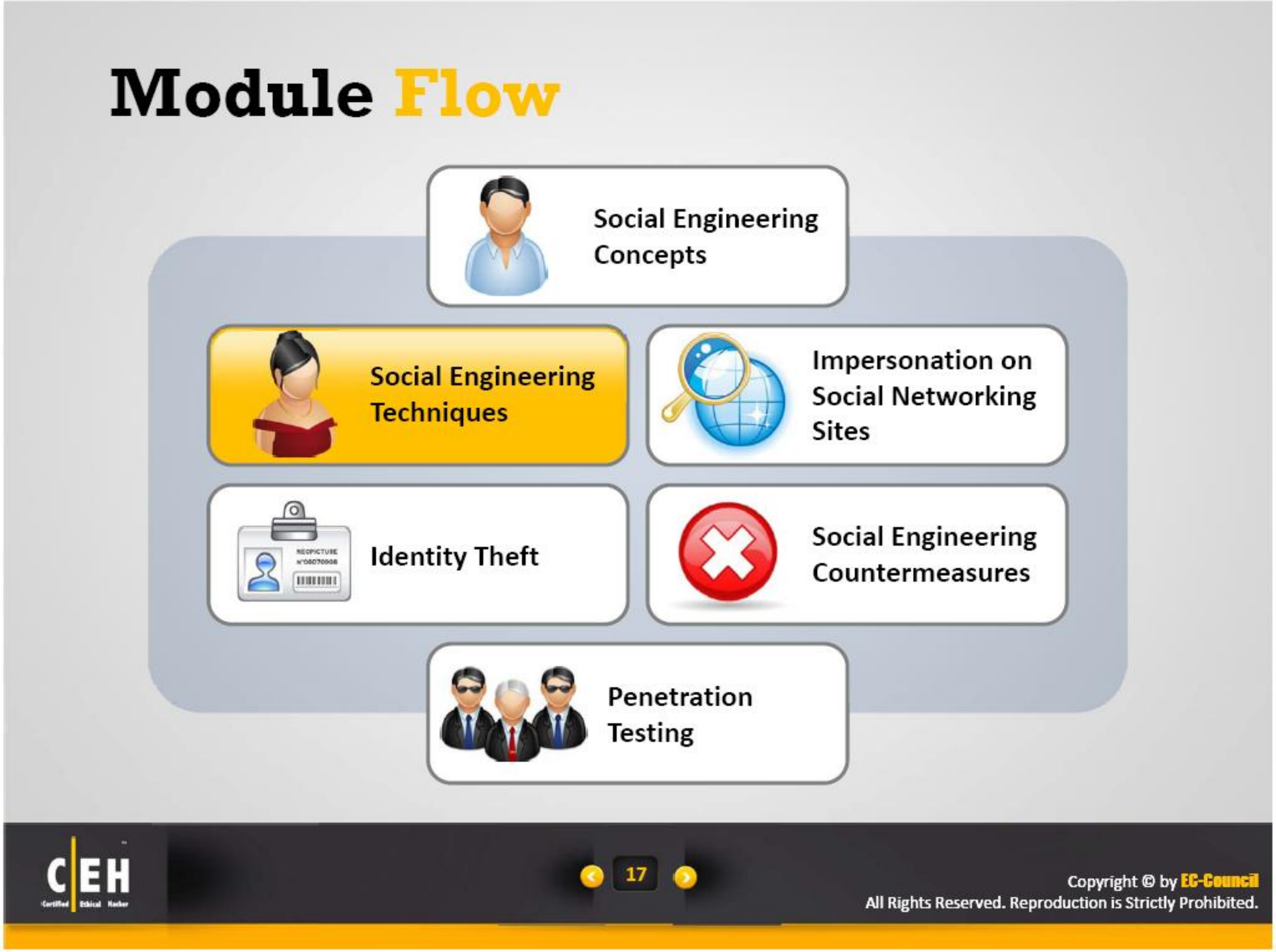
Attacker making an attempt as a valid employee to **gather information** from the staff of a company

The victim employee gives information back assuming the attacker to be a **valid employee**

Despite having the best firewall, intrusion-detection, and antivirus systems, you are still hit with security breaches

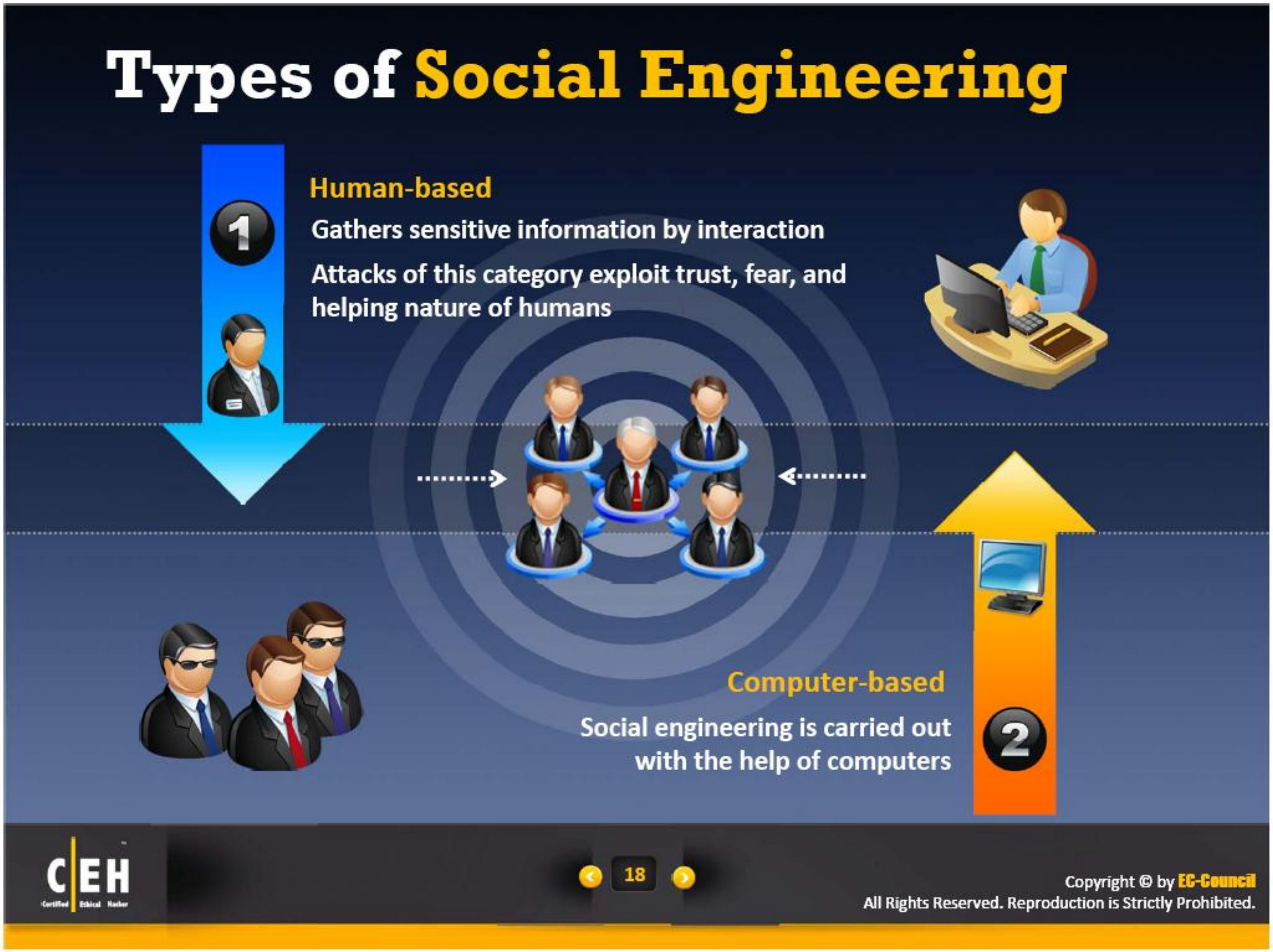
Attackers can attempt social engineering attacks on office workers to extract the sensitive data, such as:

- **Security policies**
- **Sensitive documents**
- **Office network infrastructure**
- **Passwords**



Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing



Types of Social Engineering

1

Human-based

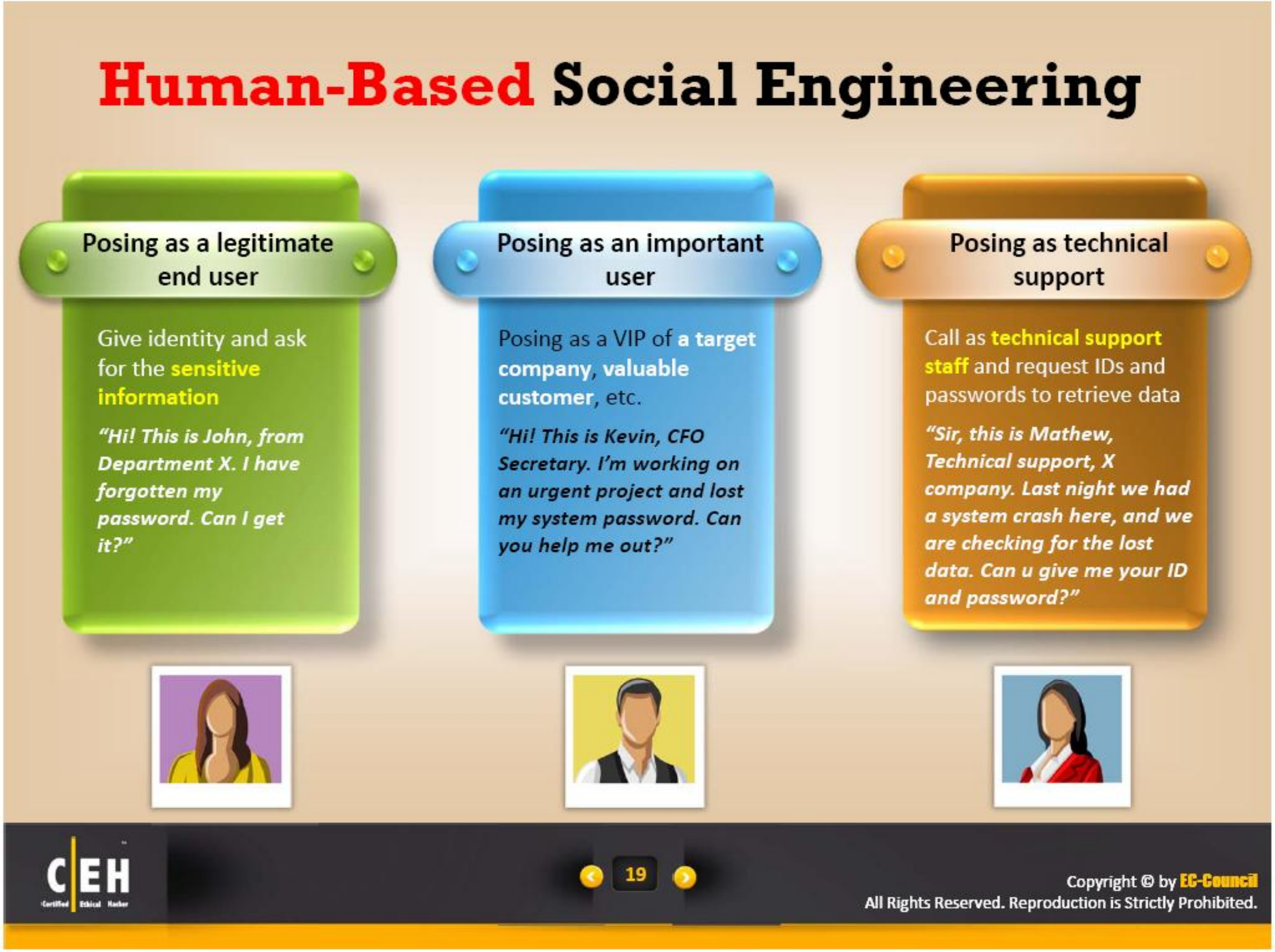
Gathers sensitive information by interaction

Attacks of this category exploit trust, fear, and helping nature of humans

2

Computer-based

Social engineering is carried out with the help of computers



Human-Based Social Engineering

Posing as a legitimate end user

Give identity and ask for the **sensitive information**

"Hi! This is John, from Department X. I have forgotten my password. Can I get it?"

Posing as an important user

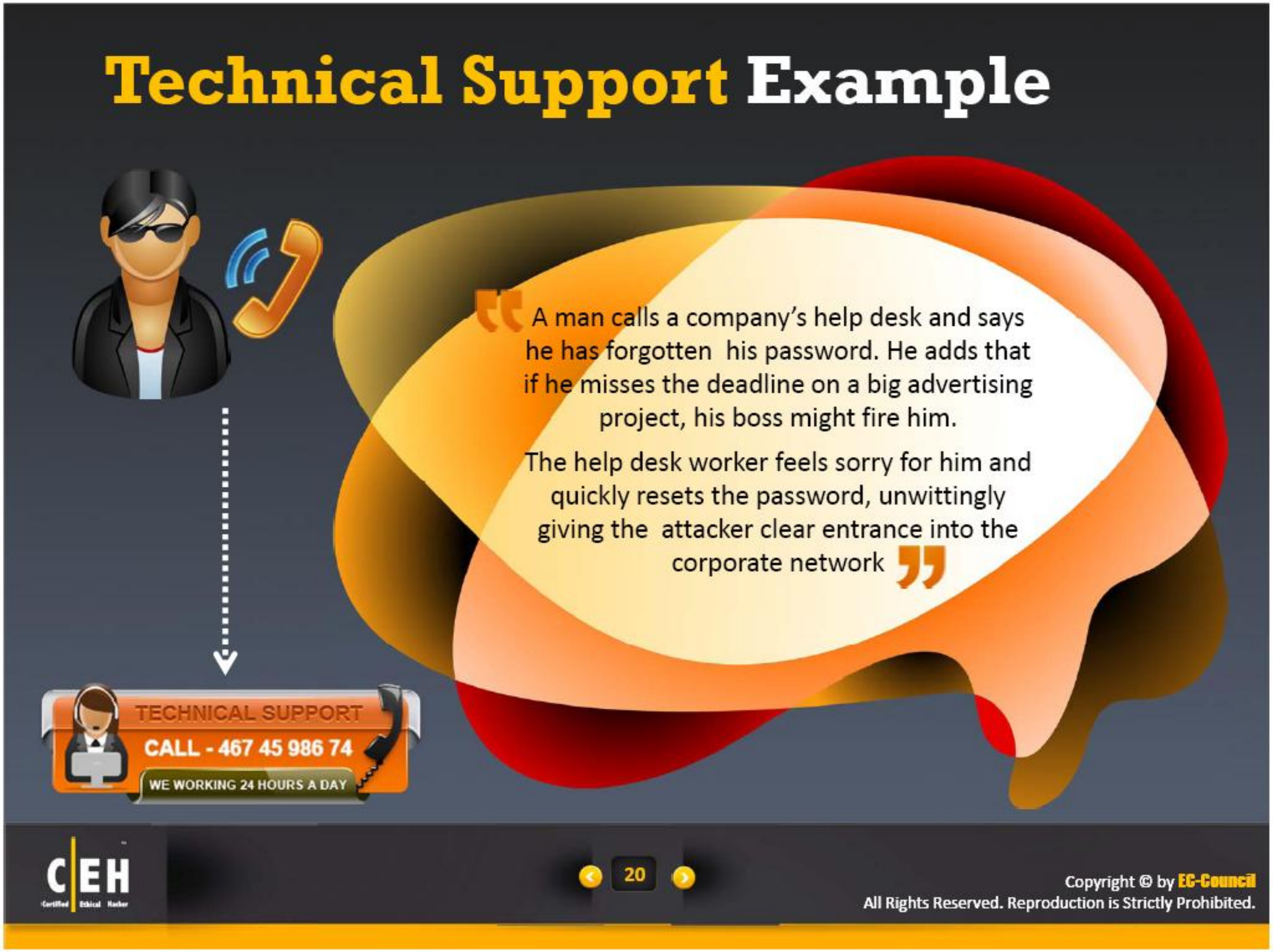
Posing as a VIP of **a target company**, **valuable customer**, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system password. Can you help me out?"

Posing as technical support

Call as **technical support staff** and request IDs and passwords to retrieve data

"Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and password?"



Technical Support Example

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

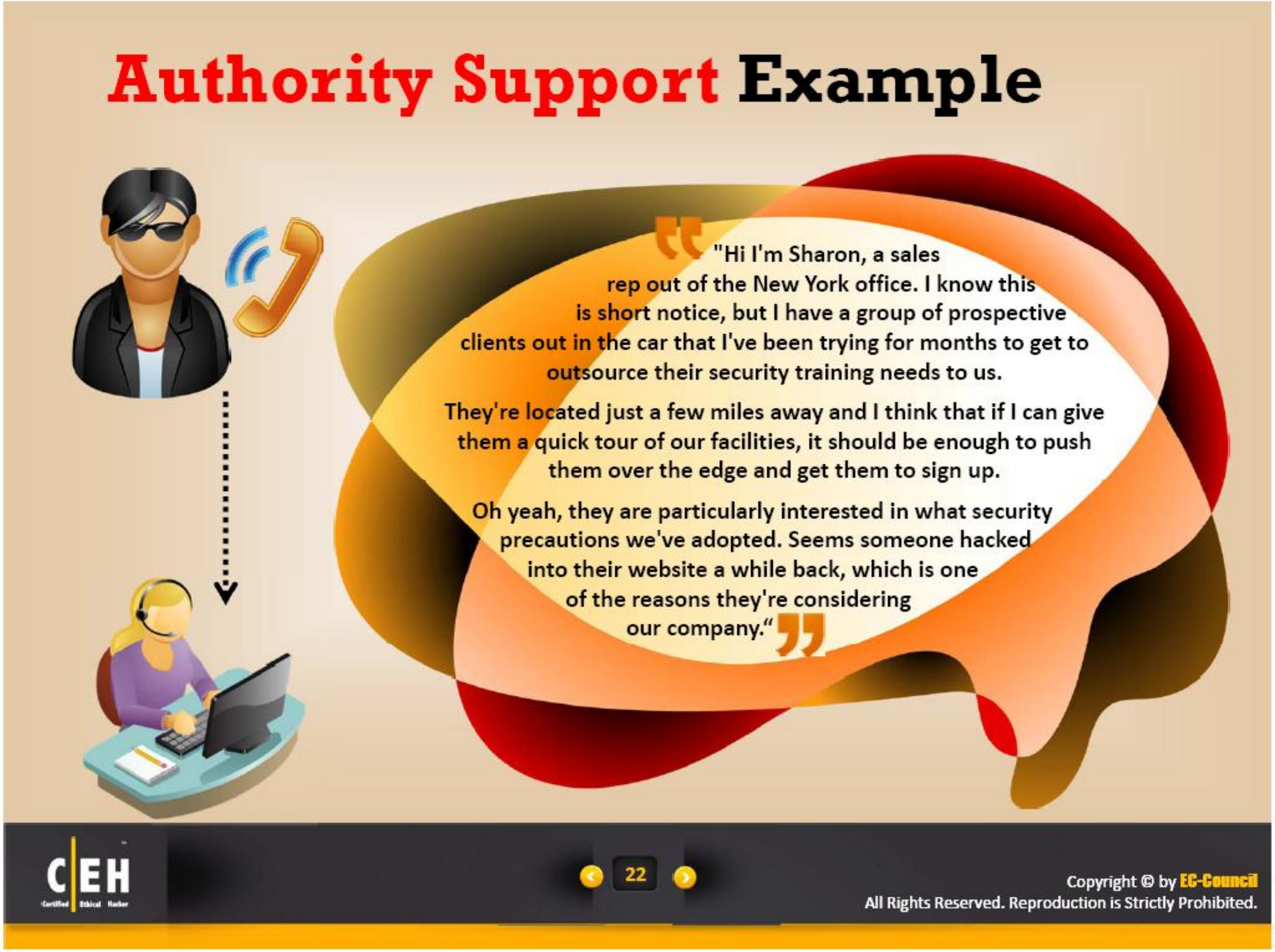
The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network"

TECHNICAL SUPPORT
CALL - 467 45 986 74
WE WORKING 24 HOURS A DAY
CEH

Authority Support Example

“Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures.

Your department has 10 minutes to show me how you would recover from a website crash.”

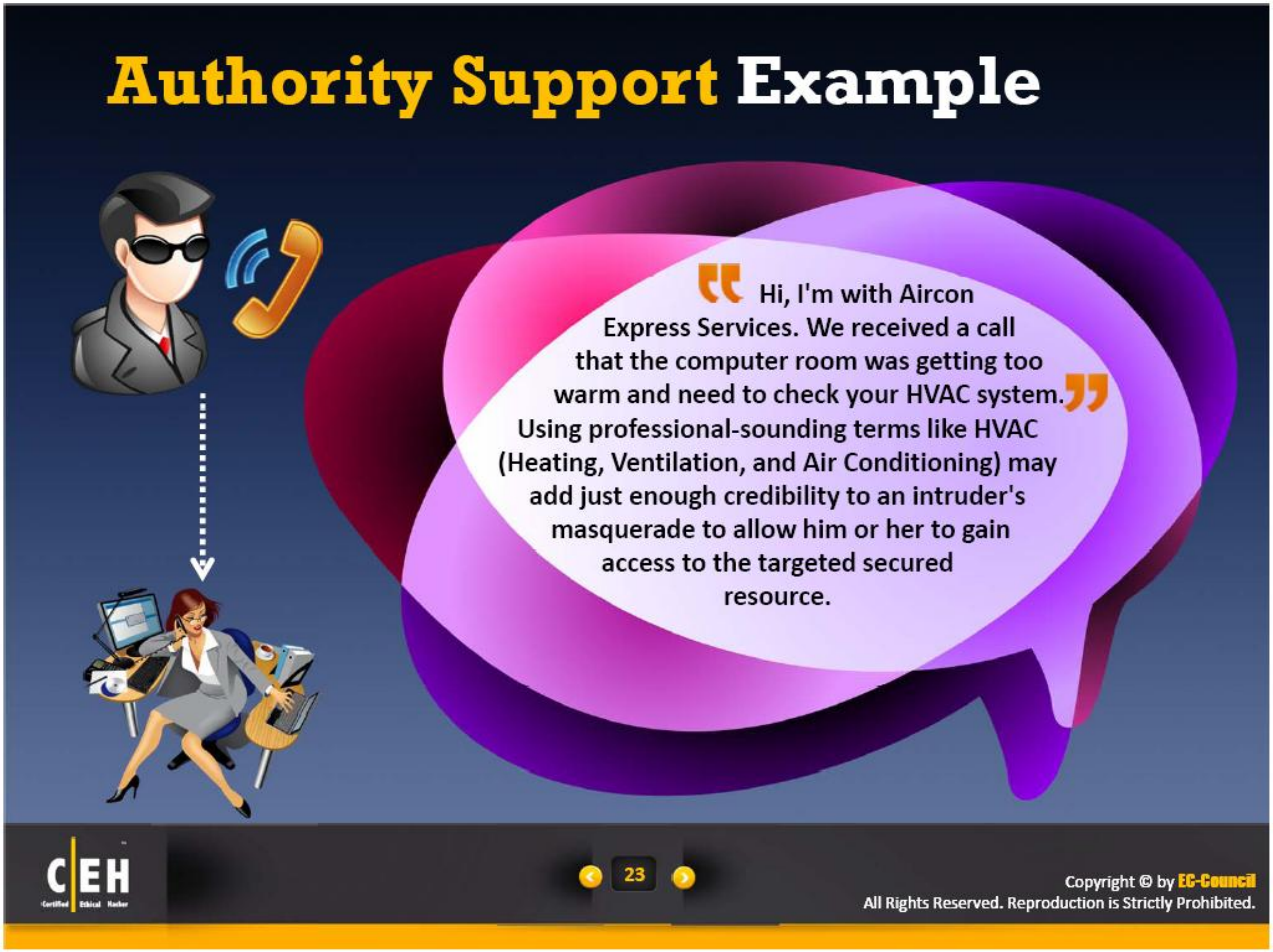


Authority Support Example

"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us.

They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

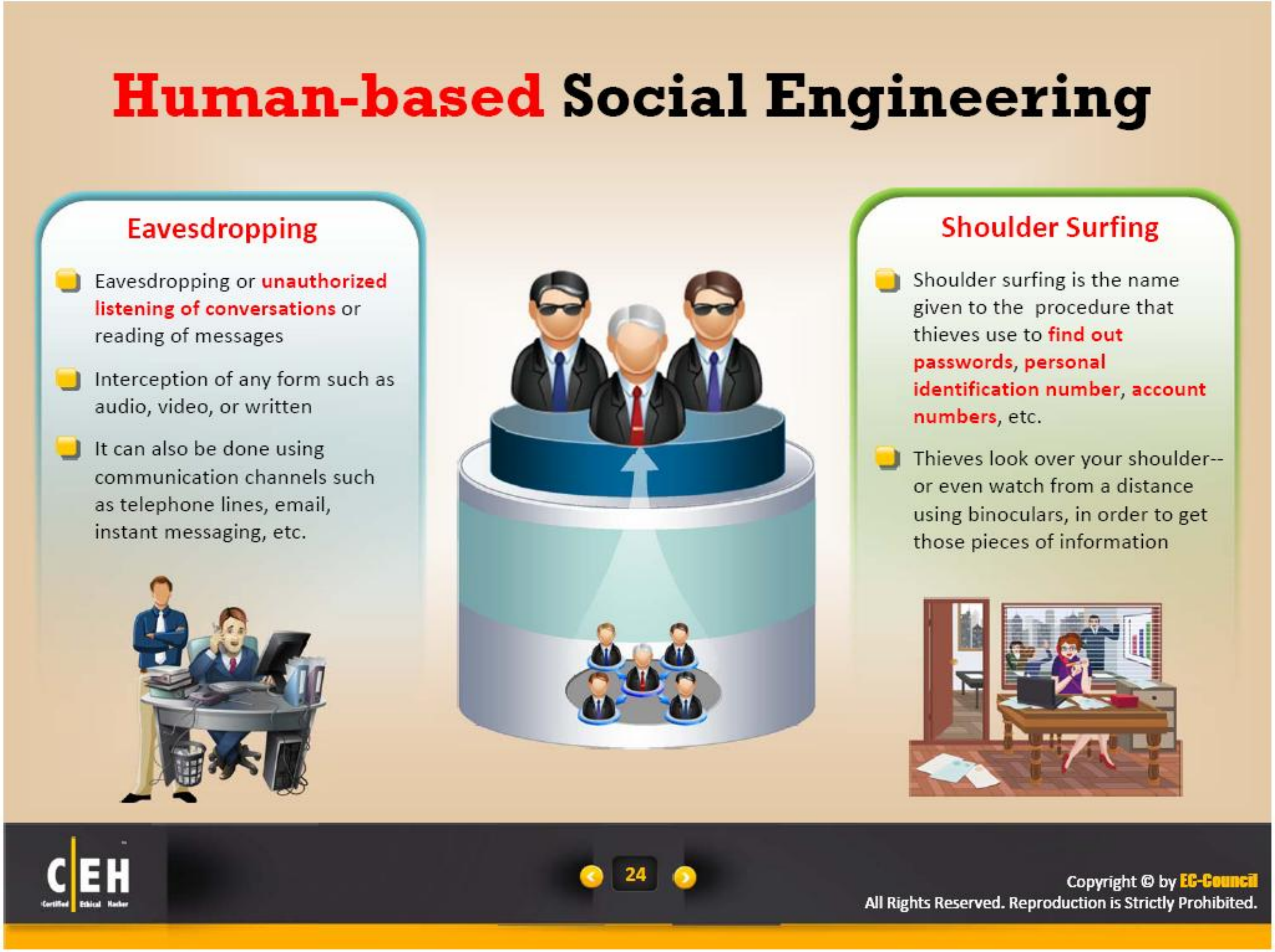
Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company.“



Authority Support Example

“Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and need to check your HVAC system.”

Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the targeted secured resource.



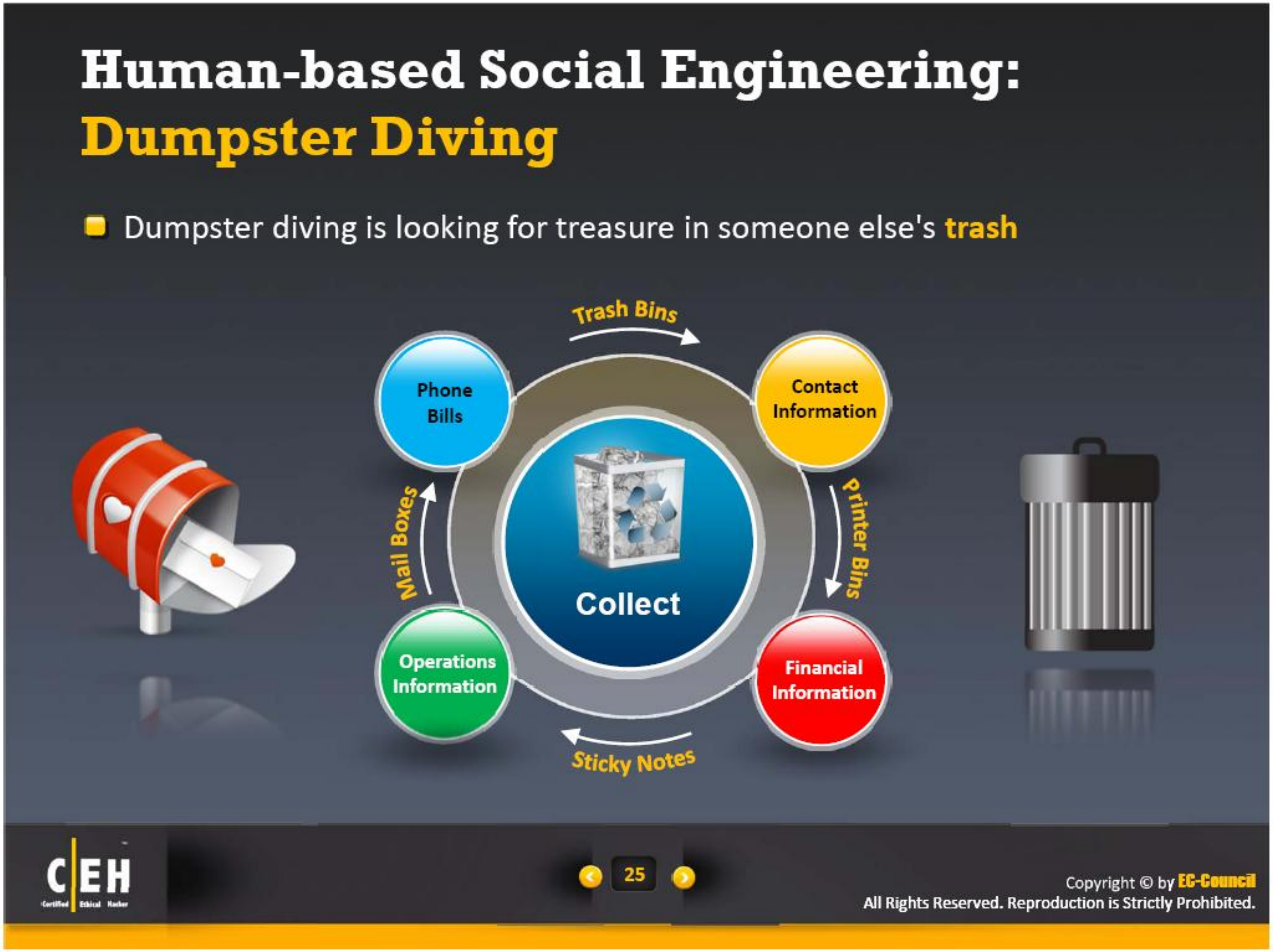
Human-based Social Engineering

Eavesdropping

- Eavesdropping or **unauthorized listening of conversations** or reading of messages
- Interception of any form such as audio, video, or written
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Shoulder surfing is the name given to the procedure that thieves use to **find out passwords**, **personal identification number**, **account numbers**, etc.
- Thieves look over your shoulder--or even watch from a distance using binoculars, in order to get those pieces of information



Human-based Social Engineering: Dumpster Diving

- Dumpster diving is looking for treasure in someone else's **trash**

Collect

Phone Bills

Trash Bins

Contact Information

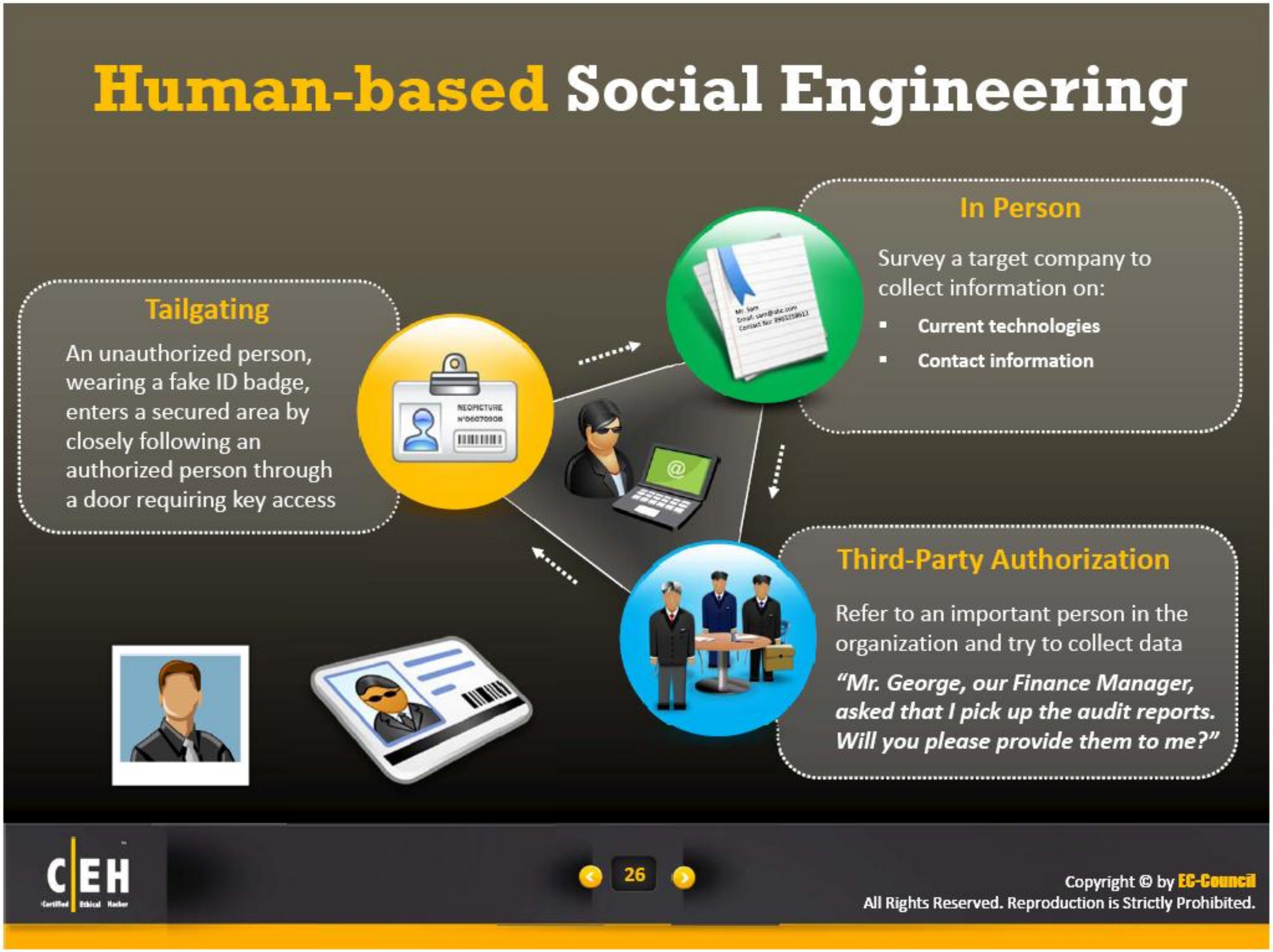
Printer Bins

Financial Information

Sticky Notes

Operations Information

Mail Boxes



Human-based Social Engineering

Tailgating

An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access

In Person

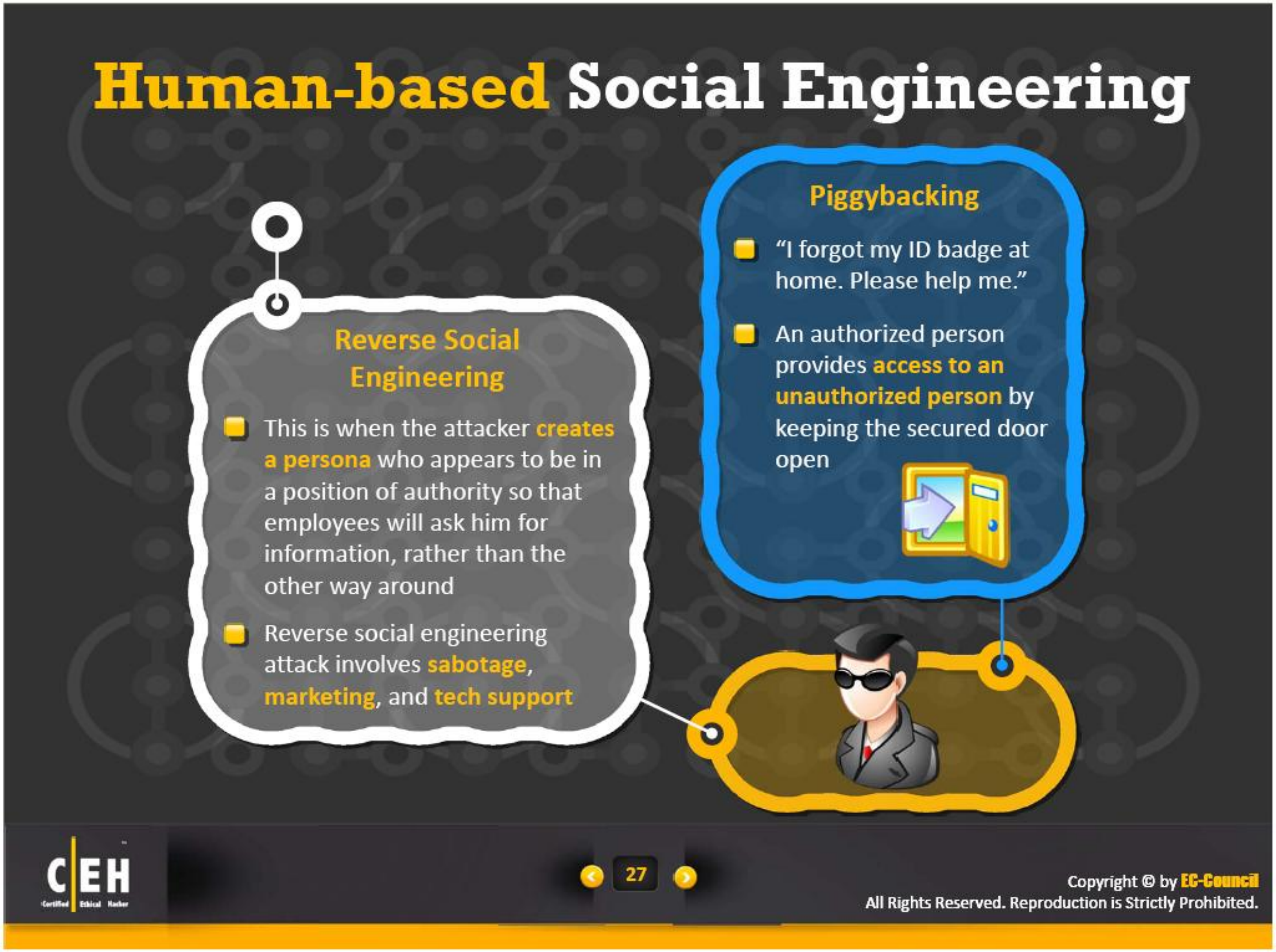
Survey a target company to collect information on:

- **Current technologies**
- **Contact information**

Third-Party Authorization

Refer to an important person in the organization and try to collect data

"Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?"



Human-based Social Engineering

Reverse Social Engineering

- This is when the attacker **creates a persona** who appears to be in a position of authority so that employees will ask him for information, rather than the other way around
- Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**

Piggybacking

- "I forgot my ID badge at home. Please help me."
- An authorized person provides **access to an unauthorized person** by keeping the secured door open

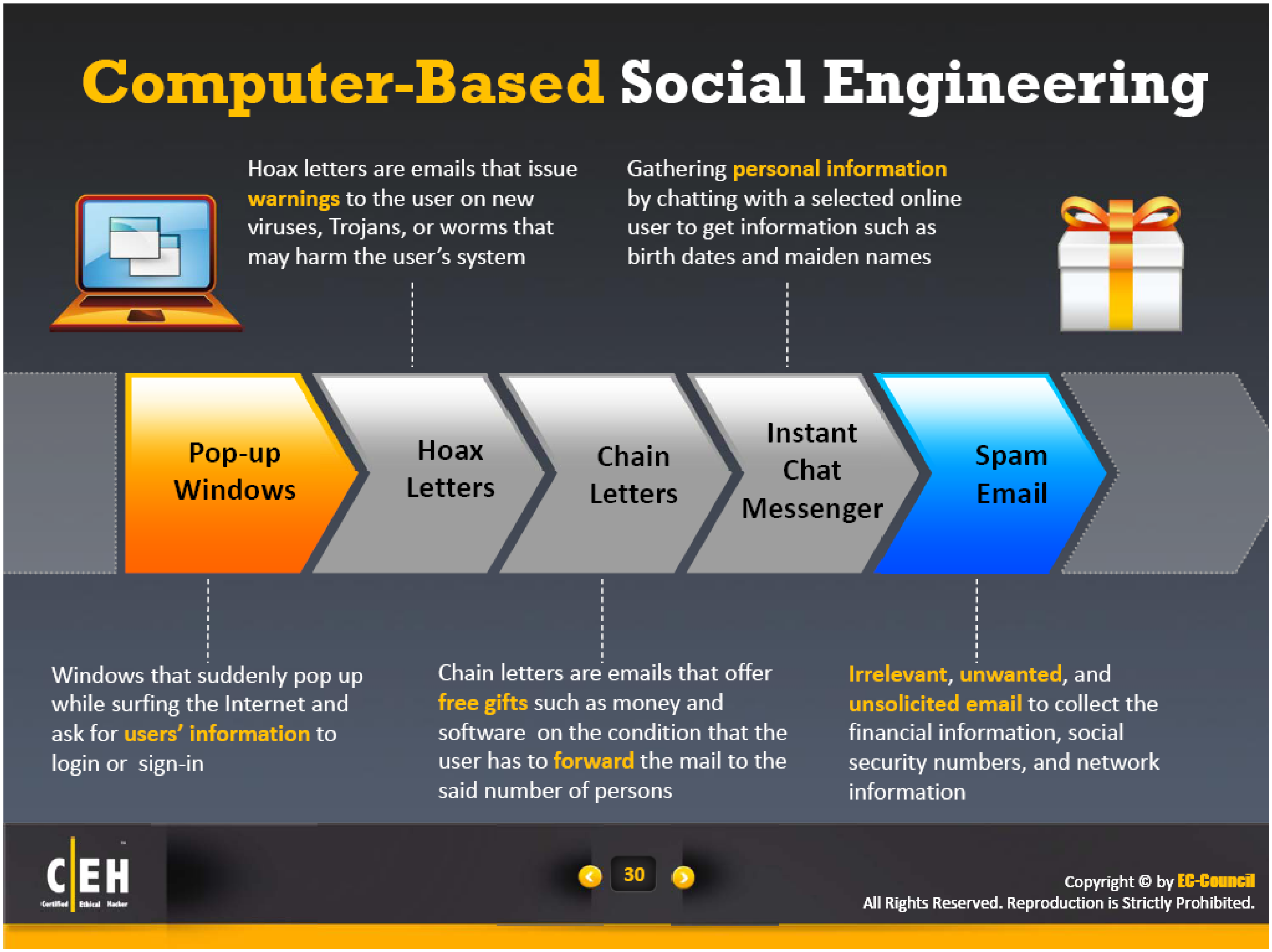
Watch these Movies

KINO AUF DER ÜBERHOLSPUR!
MARK WAHLBERG CHARLIZE THERON EDWARD NORTON
THE ITALIAN JOB
JAGD AUF MILLIONEN
leonardo dicaprio tom hanks
catch me
if you can
The true story of a real fake.

Watch this Movie

In the 2003 movie "Matchstick Men", Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water filtration systems to unsuspecting customers, in the process collecting over a million dollars

This movie is an excellent study in the art of social engineering, the act of manipulating people into performing actions or divulging confidential information



Computer-Based Social Engineering

Pop-up Windows

Hoax Letters

Chain Letters

Instant Chat Messenger

Spam Email

Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user’s system

Gathering **personal information** by chatting with a selected online user to get information such as birth dates and maiden names

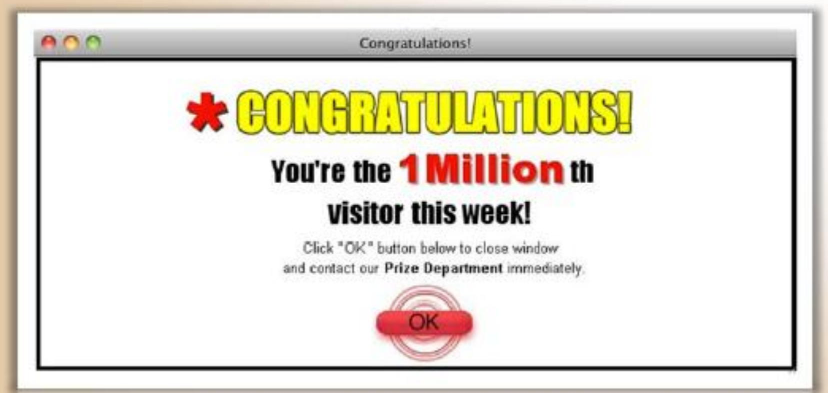
Windows that suddenly pop up while surfing the Internet and ask for **users’ information** to login or sign-in

Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward** the mail to the said number of persons

Irrelevant, **unwanted**, and **unsolicited email** to collect the financial information, social security numbers, and network information

Computer-Based Social Engineering: Pop-Ups

- Pop-ups trick users into **clicking a hyperlink** that redirects them to **fake web pages** asking for personal information, or downloads malicious programs such keyloggers, Trojans, or spyware

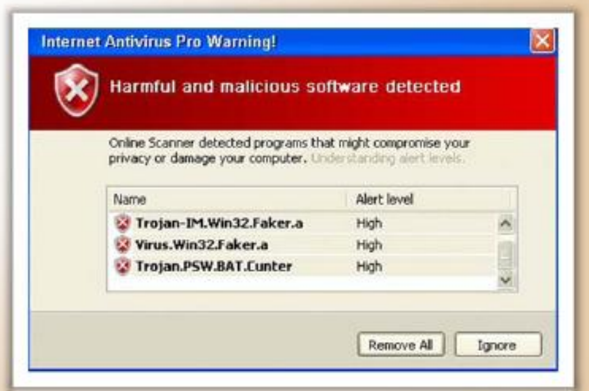


Congratulations!

CONGRATULATIONS!

You're the 1 Million th visitor this week!

Click "OK" button below to close window and contact our **Prize Department** immediately.



Internet Antivirus Pro Warning!

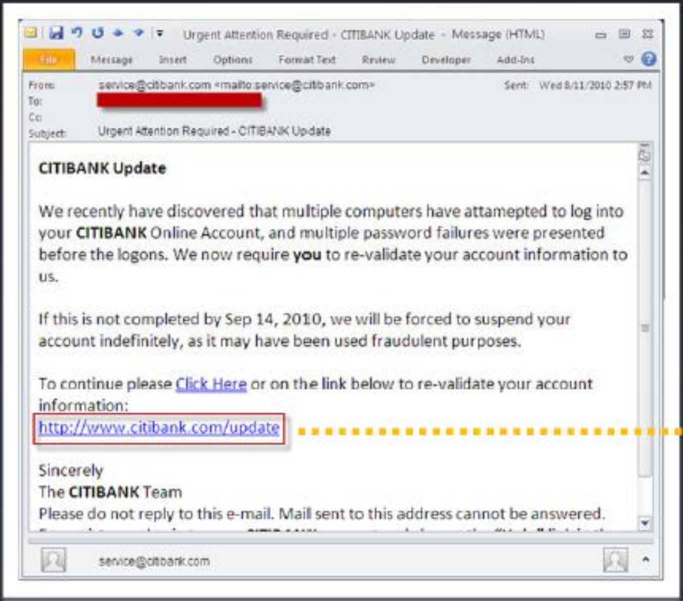
Harmful and malicious software detected

Online Scanner detected programs that might compromise your privacy or damage your computer. Understanding alert levels.

Name	Alert level
Trojan-IM.Win32.Faker.a	High
Virus.Win32.Faker.a	High
Trojan.PSW.BAT.Cunter	High

Computer-Based Social Engineering: Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information
- Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information


Urgent Attention Required - CITIBANK Update - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Developer
Add-Ins

From: service@citibank.com <mailto:service@citibank.com>   Sent: Wed 8/11/2010 2:57 PM
To: [redacted]
Cc:
Subject: Urgent Attention Required - CITIBANK Update

CITIBANK Update

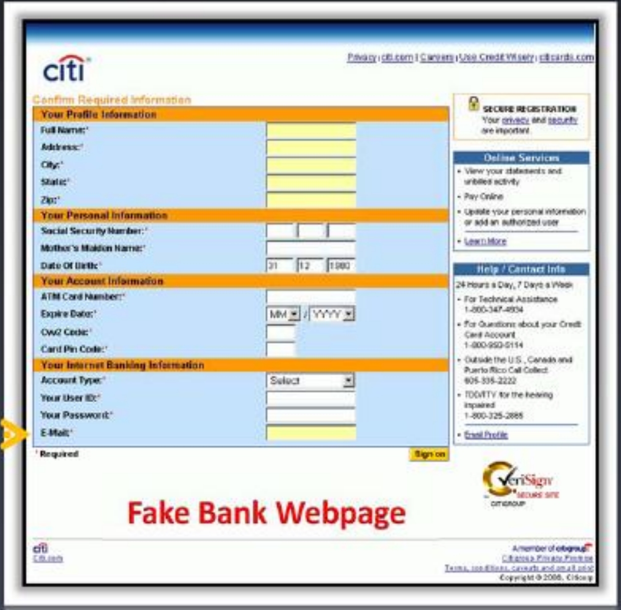
We recently have discovered that multiple computers have attamepted to log into your **CITIBANK** Online Account, and multiple password failures were presented before the logons. We now require **you** to re-validate your account information to us.

If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

To continue please Click Here or on the link below to re-validate your account information:
http://www.citibank.com/update

Sincerely
The **CITIBANK** Team
Please do not reply to this e-mail. Mail sent to this address cannot be answered.

service@citibank.com


citi
Privacy | citi.com | Careers | Use Credit Wisely | citicards.com

Confirm Required Information

Your Profile Information
Full Name:*
Address:*
City:*
State:*
Zip:*

Your Personal Information
Social Security Number:*
Mother's Maiden Name:*
Date Of Birth:* 31 12 1980

Your Account Information
ATM Card Number:*
Expire Date:* MM / YYYY
Cvv2 Code:*
Card Pin Code:*

Your Internet Banking Information
Account Type:* Select
Your User ID:*
Your Password:*
E-Mail:*

* Required

Sign on

SECURE REGISTRATION
Your privacy and security are important

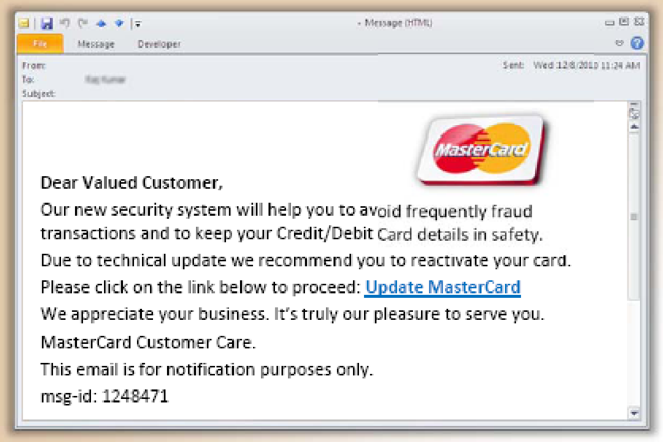
Online Services
- View your statements and unbilled activity
- Pay Online
- Update your personal information or add an authorized user
- Learn More

Help / Contact Info
24 Hours a Day, 7 Days a Week
- For Technical Assistance 1-800-347-4934
- For Questions about your Credit Card Account 1-800-950-5114
- Outside the U.S., Canada and Puerto Rico Call Collect 605-335-2222
- TDD/TTY for the hearing impaired 1-800-325-2865
- Email Profile

A member of citigroup
Citigroup Privacy Promise
Terms, conditions, caveats and small print
Copyright © 2006, Citicorp

Fake Bank Webpage

Computer-Based Social Engineering: Phishing



From:
To: Raj Kumar
Subject:
Sent: Wed 12/8/2010 11:24 AM

Dear Valued Customer,

Our new security system will help you to avoid frequently fraud transactions and to keep your Credit/Debit Card details in safety.

Due to technical update we recommend you to reactivate your card.

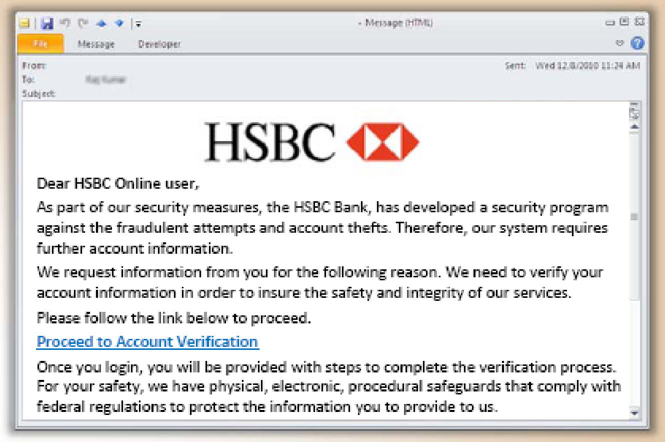
Please click on the link below to proceed: Update MasterCard

We appreciate your business. It's truly our pleasure to serve you.

MasterCard Customer Care.

This email is for notification purposes only.

msg-id: 1248471



From:
To: Raj Kumar
Subject:
Sent: Wed 12/8/2010 11:24 AM

Dear HSBC Online user,

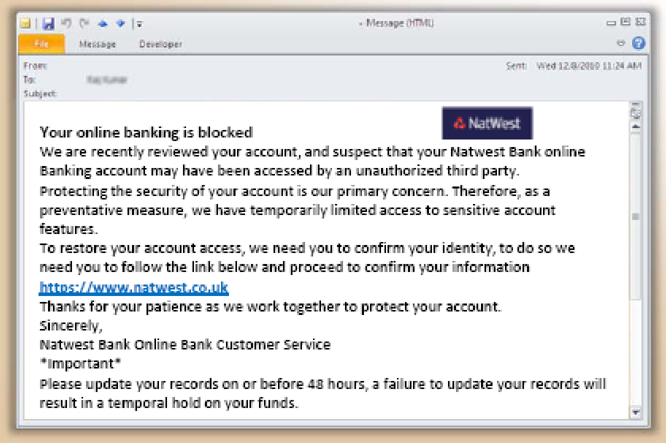
As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information.

We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

Please follow the link below to proceed.

Proceed to Account Verification

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.



From:
To: Raj Kumar
Subject:
Sent: Wed 12/8/2010 11:24 AM

Your online banking is blocked

We are recently reviewed your account, and suspect that your Natwest Bank online Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity, to do so we need you to follow the link below and proceed to confirm your information

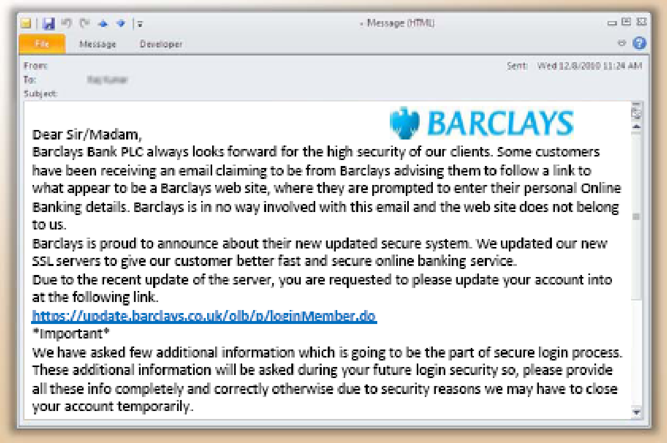
https://www.natwest.co.uk

Thanks for your patience as we work together to protect your account.

Sincerely,
Natwest Bank Online Bank Customer Service

Important

Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.



From:
To: Raj Kumar
Subject:
Sent: Wed 12/8/2010 11:24 AM

Dear Sir/Madam,

Barclays Bank PLC always looks forward for the high security of our clients. Some customers have been receiving an email claiming to be from Barclays advising them to follow a link to what appear to be a Barclays web site, where they are prompted to enter their personal Online Banking details. Barclays is in no way involved with this email and the web site does not belong to us.

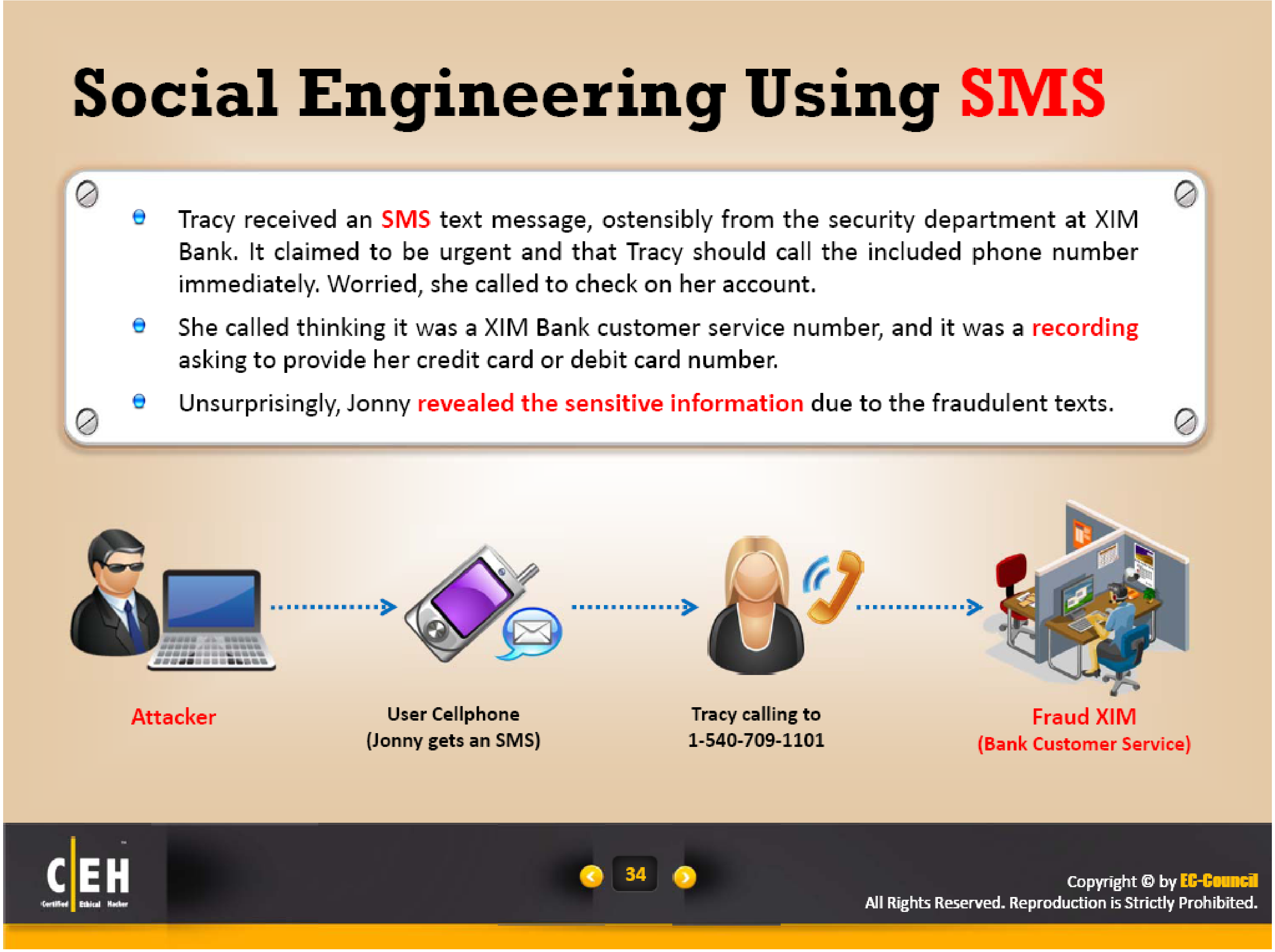
Barclays is proud to announce about their new updated secure system. We updated our new SSL servers to give our customer better fast and secure online banking service.

Due to the recent update of the server, you are requested to please update your account into at the following link.

https://update.barclays.co.uk/olb/p/loginMember.do

Important

We have asked few additional information which is going to be the part of secure login process. These additional information will be asked during your future login security so, please provide all these info completely and correctly otherwise due to security reasons we may have to close your account temporarily.



Social Engineering Using SMS

- Tracy received an SMS text message, ostensibly from the security department at XIM Bank. It claimed to be urgent and that Tracy should call the included phone number immediately. Worried, she called to check on her account.
- She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number.
- Unsurprisingly, Jonny revealed the sensitive information due to the fraudulent texts.

Attacker

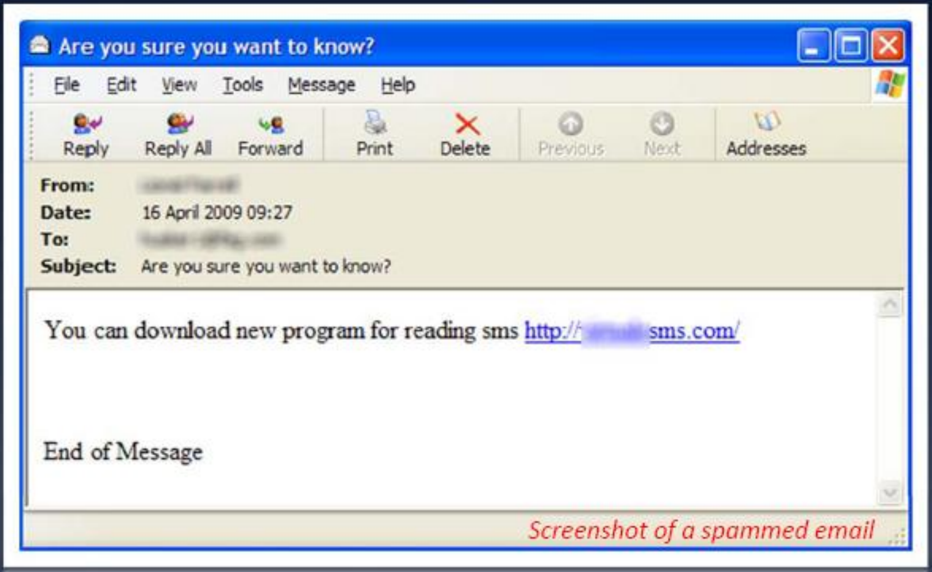
User Cellphone
(Jonny gets an SMS)

Tracy calling to
1-540-709-1101

Fraud XIM
(Bank Customer Service)

Social Engineering by a "Fake SMS Spying Tool"

- The users are enticed to download an application that will permit them to view other people's SMS messages online
- The download file uses alternating filenames, including sms.exe, freetrial.exe, and smstrap.exe

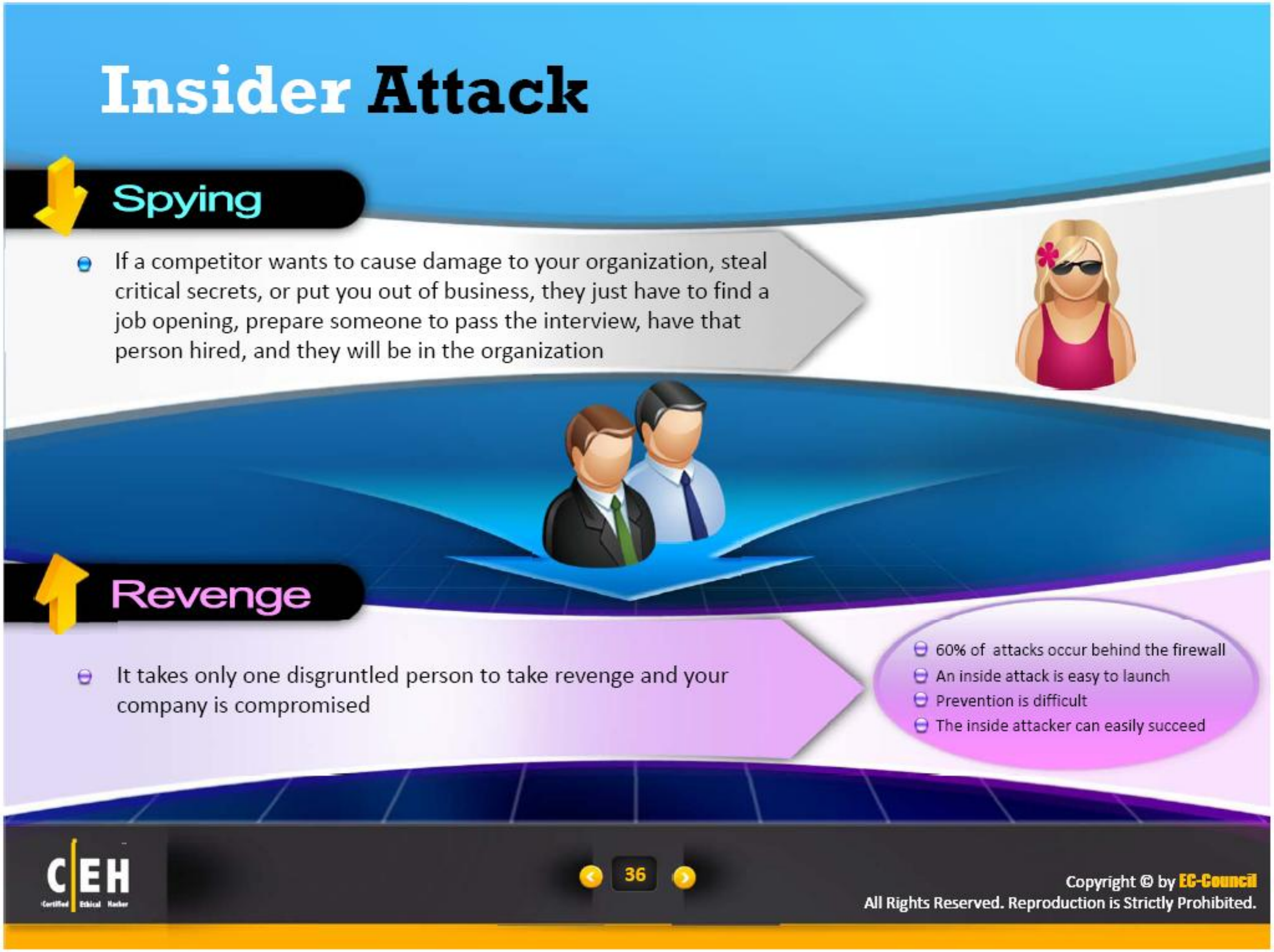

Are you sure you want to know?
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: [redacted]
Date: 16 April 2009 09:27
To: [redacted]
Subject: Are you sure you want to know?

You can download new program for reading sms http://[redacted]sms.com/

End of Message

Screenshot of a spammed email



Insider Attack

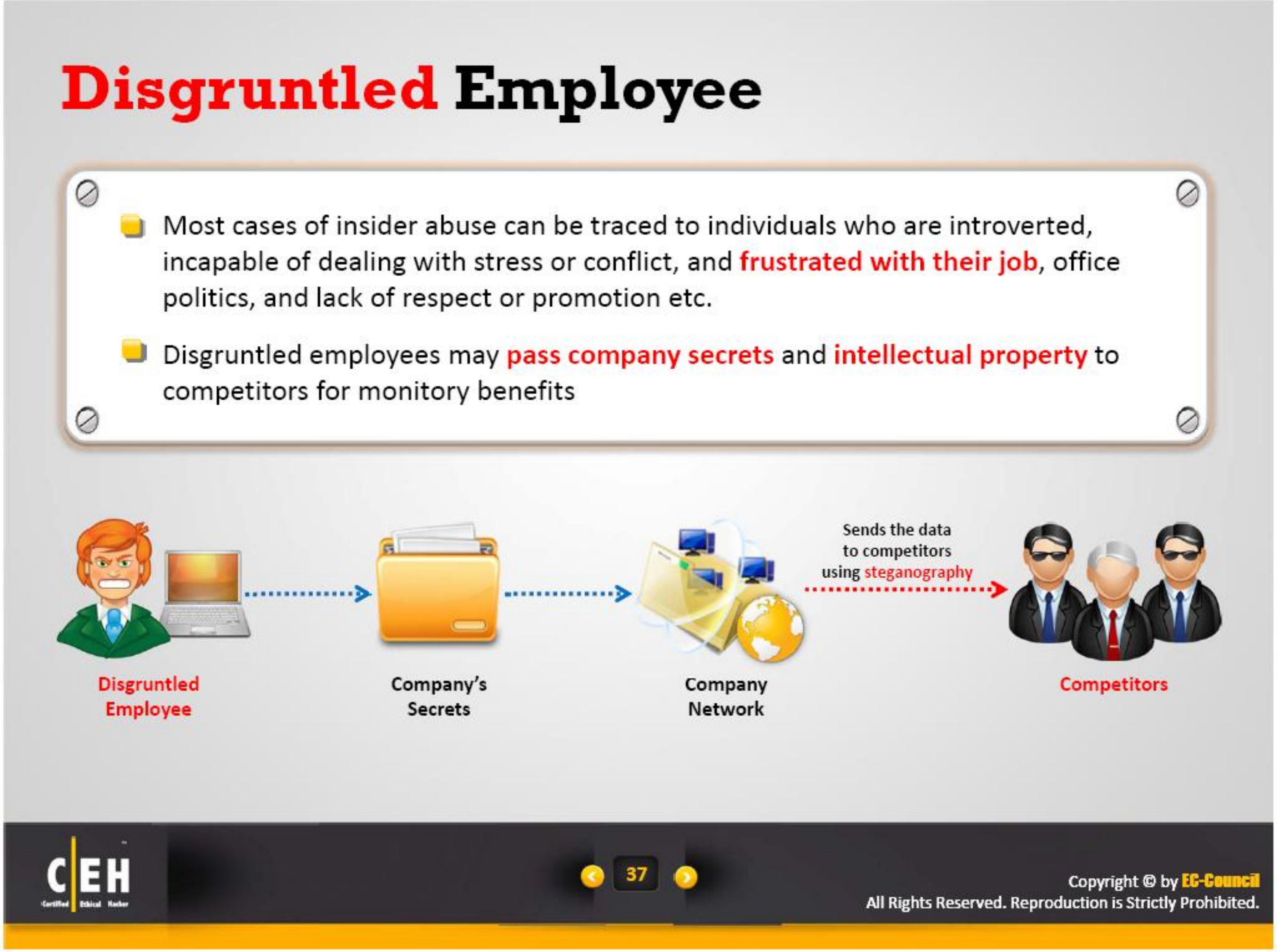
Spying

- If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization

Revenge

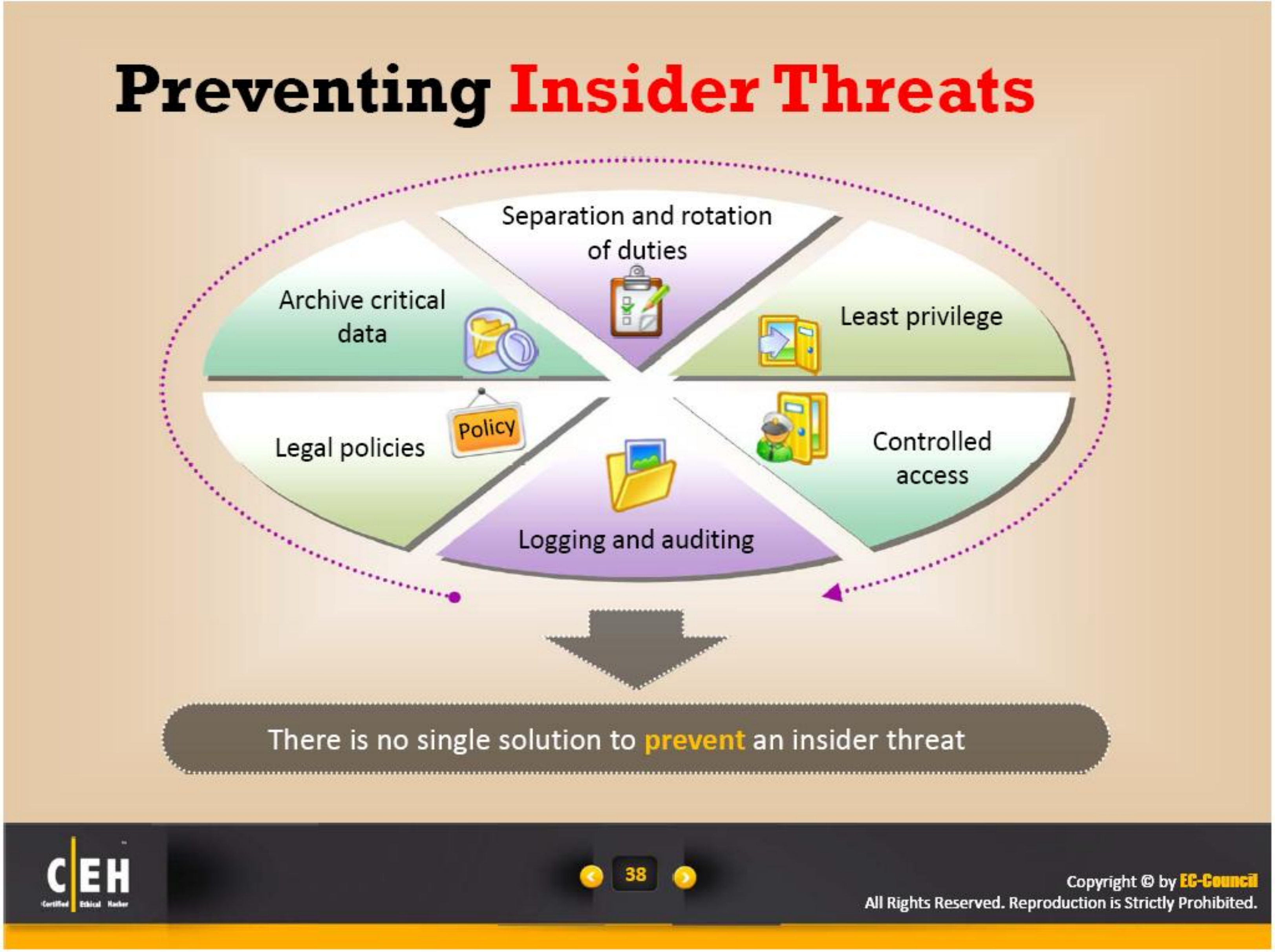
- It takes only one disgruntled person to take revenge and your company is compromised

- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed



Disgruntled Employee

- Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and **frustrated with their job**, office politics, and lack of respect or promotion etc.
- Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monitory benefits



Preventing Insider Threats

Separation and rotation of duties

Archive critical data

Least privilege

Legal policies

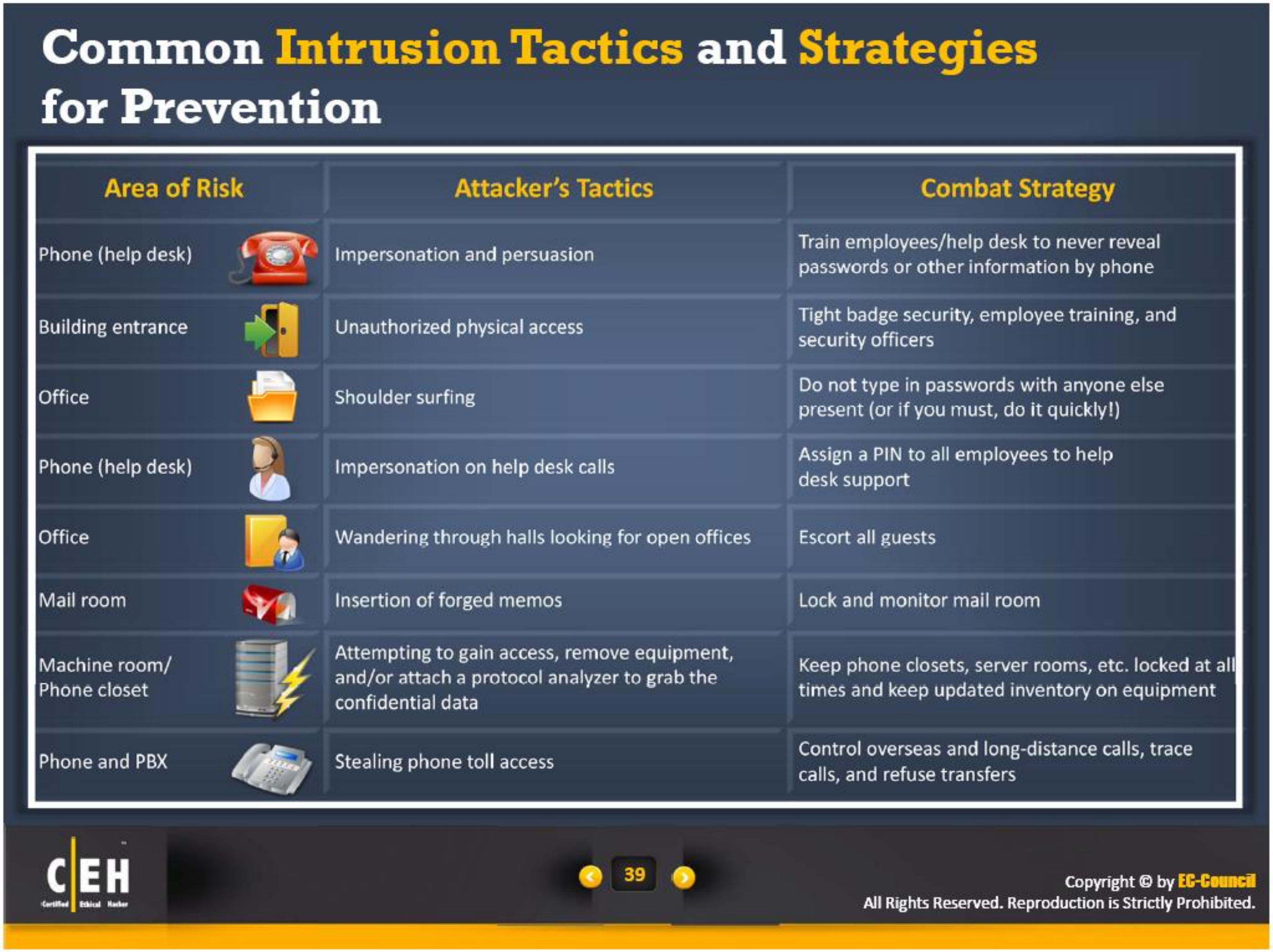
Policy

Controlled access

Logging and auditing

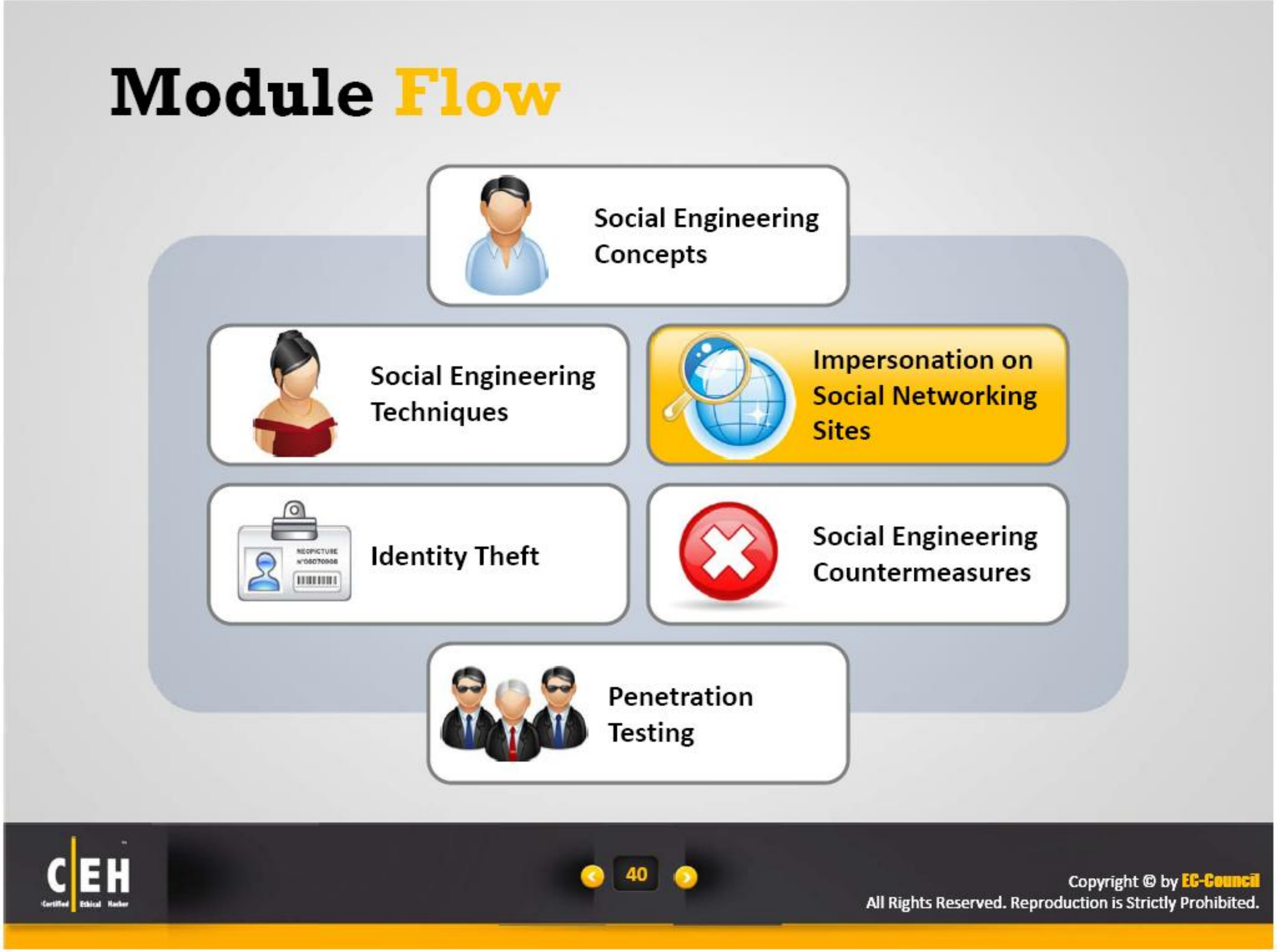
There is no single solution to **prevent** an insider threat

CEH



Common Intrusion Tactics and Strategies for Prevention

Area of Risk	Attacker's Tactics	Combat Strategy
Phone (help desk)	Impersonation and persuasion	Train employees/help desk to never reveal passwords or other information by phone
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers
Office	Shoulder surfing	Do not type in passwords with anyone else present (or if you must, do it quickly!)
Phone (help desk)	Impersonation on help desk calls	Assign a PIN to all employees to help desk support
Office	Wandering through halls looking for open offices	Escort all guests
Mail room	Insertion of forged memos	Lock and monitor mail room
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Phone and PBX	Stealing phone toll access	Control overseas and long-distance calls, trace calls, and refuse transfers



Module Flow

Social Engineering Concepts

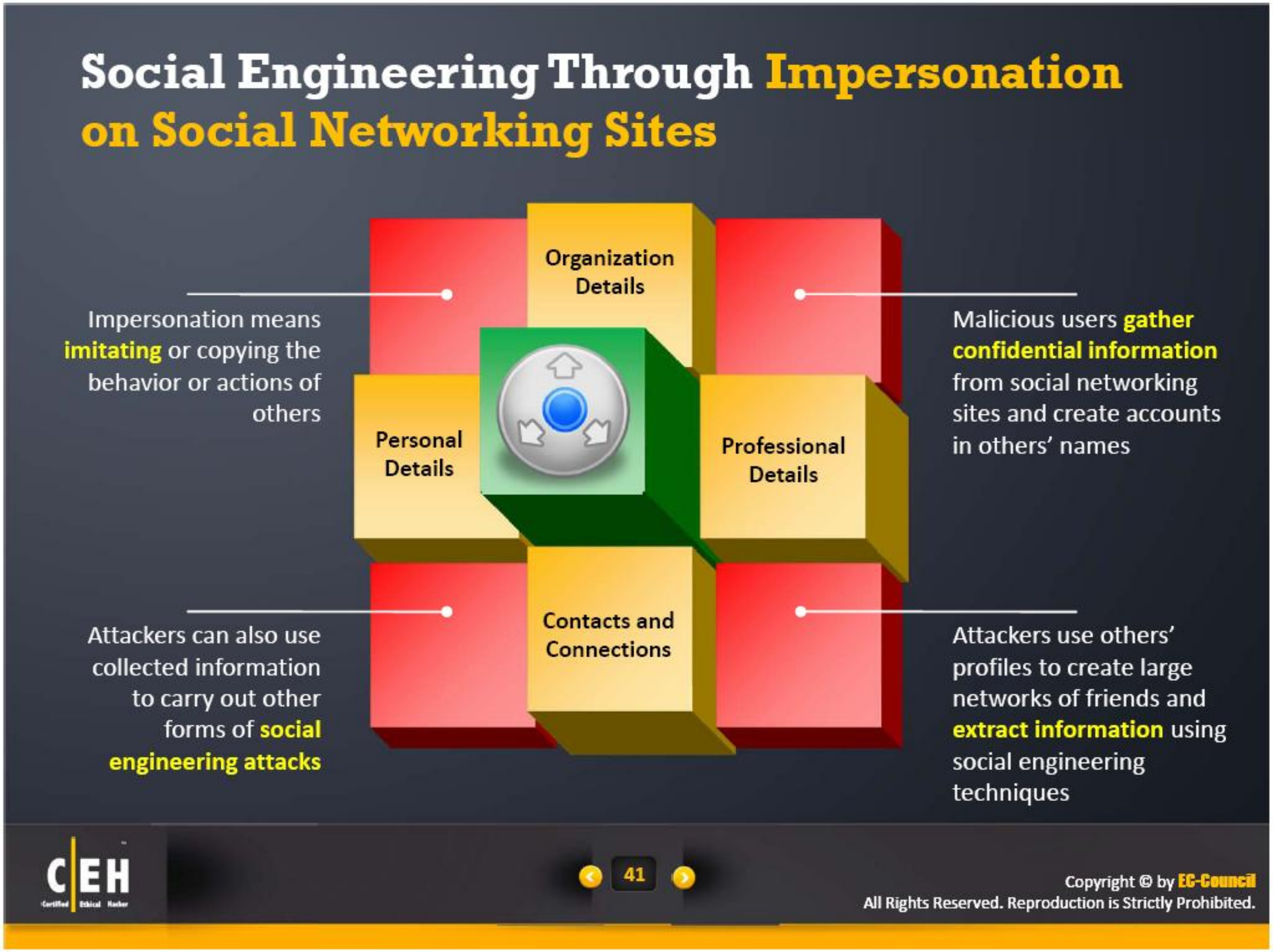
Social Engineering Techniques

Impersonation on Social Networking Sites

Identity Theft

Social Engineering Countermeasures

Penetration Testing



Social Engineering Through Impersonation on Social Networking Sites

Organization Details

Personal Details

Professional Details

Contacts and Connections

Impersonation means **imitating** or copying the behavior or actions of others

Malicious users **gather confidential information** from social networking sites and create accounts in others' names

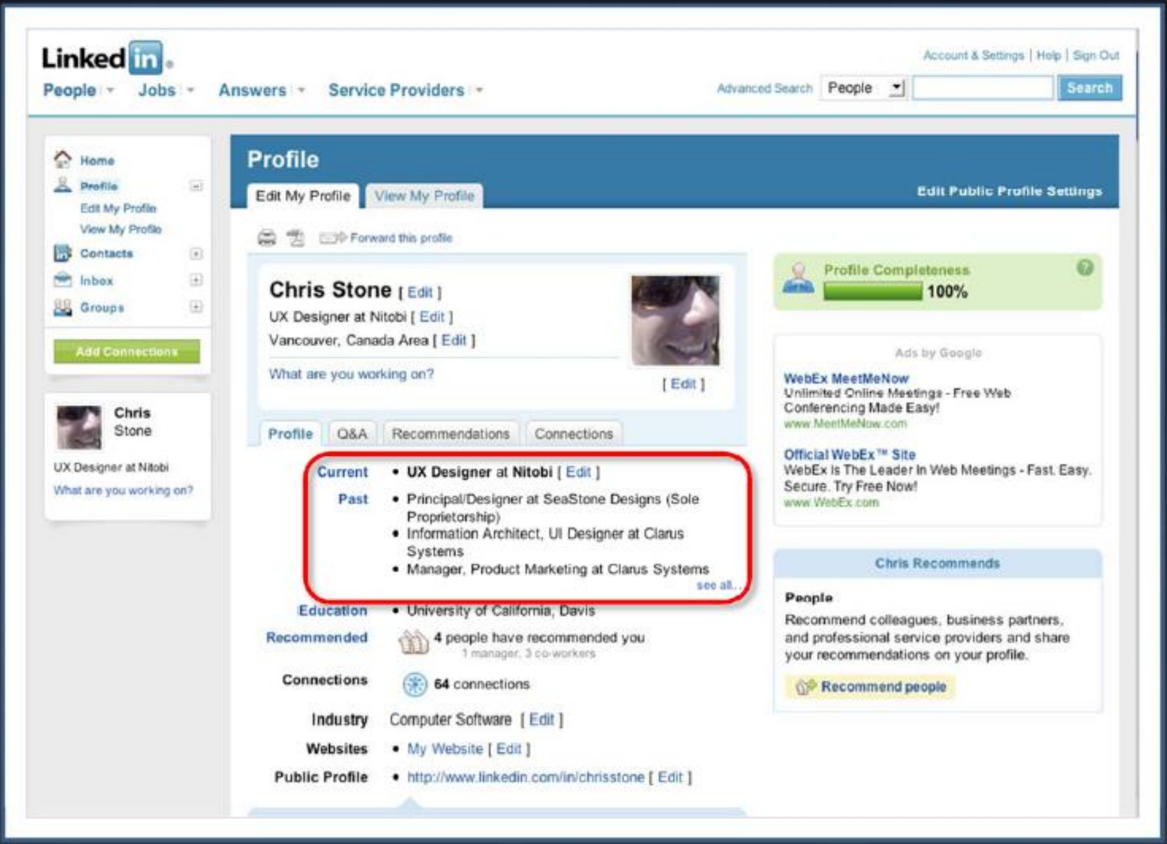
Attackers can also use collected information to carry out other forms of **social engineering attacks**

Attackers use others' profiles to create large networks of friends and **extract information** using social engineering techniques

C|EH Certified Ethical Hacker

41

Social Engineering Example: LinkedIn Profile



Profile

Chris Stone [Edit]
UX Designer at Nitobi [Edit]
Vancouver, Canada Area [Edit]
What are you working on?
[Edit]

Chris Stone
UX Designer at Nitobi
What are you working on?

Current	• UX Designer at Nitobi [Edit]
Past	• Principal/Designer at SeaStone Designs (Sole Proprietorship) • Information Architect, UI Designer at Clarus Systems • Manager, Product Marketing at Clarus Systems see all...
Education	• University of California, Davis
Recommended	4 people have recommended you 1 manager, 3 co-workers
Connections	64 connections
Industry	Computer Software [Edit]
Websites	• My Website [Edit]
Public Profile	• http://www.linkedin.com/in/chrisstone [Edit]

Profile Completeness 100%

Ads by Google

WebEx MeetMeNow
Unlimited Online Meetings - Free Web Conferencing Made Easy!
www.MeetMeNow.com

Official WebEx™ Site
WebEx Is The Leader In Web Meetings - Fast, Easy, Secure. Try Free Now!
www.WebEx.com

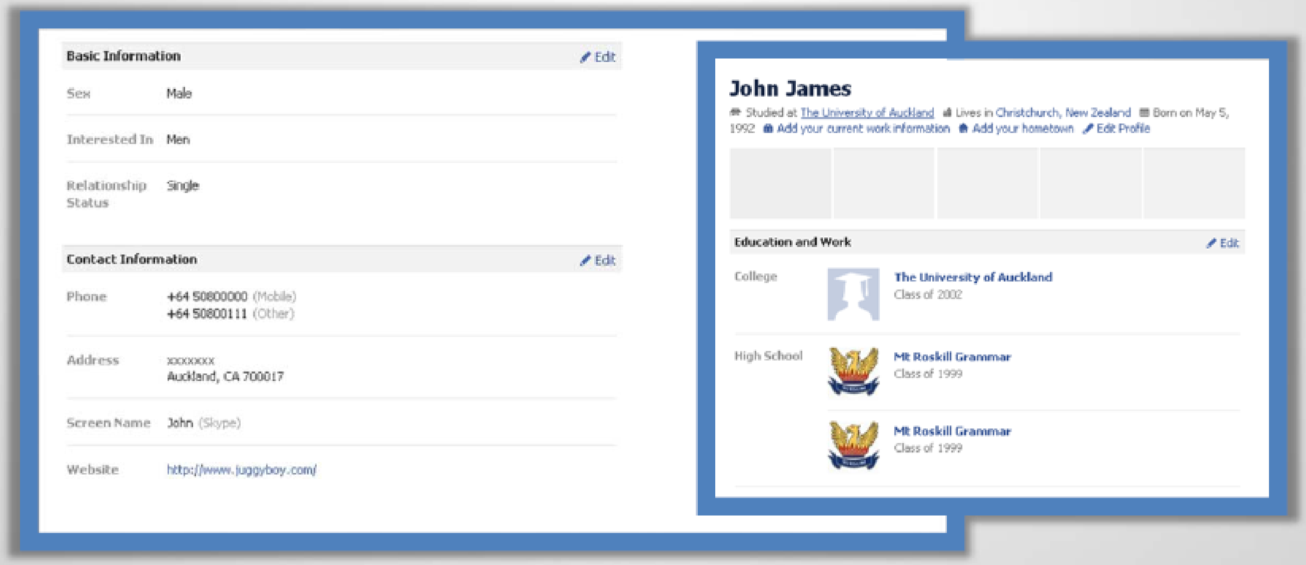
Chris Recommends

People
Recommend colleagues, business partners, and professional service providers and share your recommendations on your profile.

CEH Certified Ethical Hacker

Social Engineering on Facebook

- Attackers create a **fake user group** on Facebook identified as "Employees of" the company
- Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group, " Employees of the company"
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can **compromise** a secured facility to **gain access** to the building



Basic Information ✎ Edit

Sex	Male
Interested In	Men
Relationship Status	Single

Contact Information ✎ Edit

Phone	+64 50800000 (Mobile) +64 50800111 (Other)
Address	xxxxxxx Auckland, CA 700017
Screen Name	John (Skype)
Website	http://www.juggyboy.com/

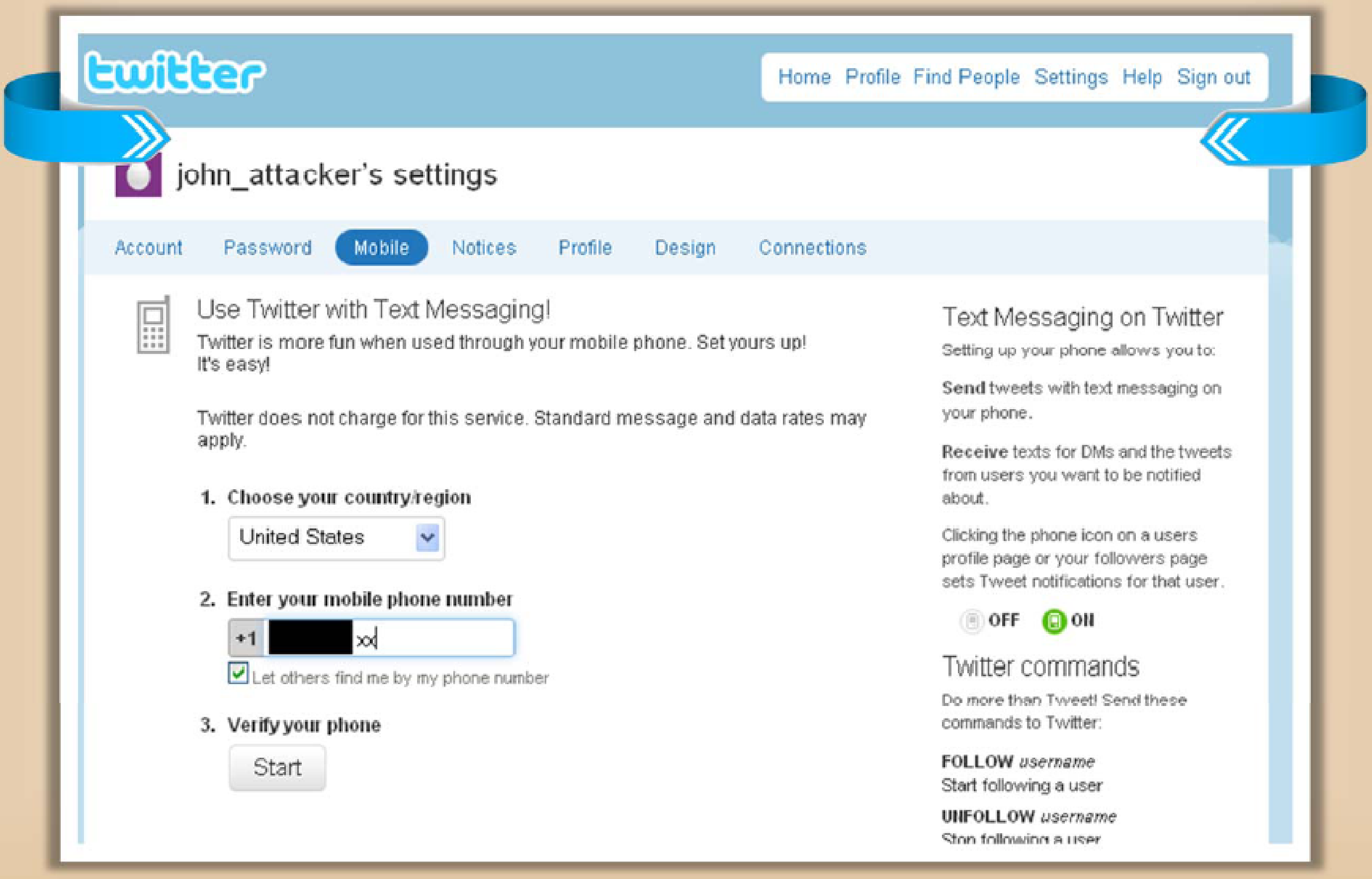
John James

Studied at The University of Auckland · Lives in Christchurch, New Zealand · Born on May 5, 1992 · Add your current work information · Add your hometown · ✎ Edit Profile

Education and Work ✎ Edit

College	The University of Auckland Class of 2002
High School	Mt Roskill Grammar Class of 1999
	Mt Roskill Grammar Class of 1999

Social Engineering on Twitter



twitter
Home Profile Find People Settings Help Sign out

john_attacker's settings

Account Password Mobile Notices Profile Design Connections

Use Twitter with Text Messaging!

Twitter is more fun when used through your mobile phone. Set yours up! It's easy!

Twitter does not charge for this service. Standard message and data rates may apply.

1. Choose your country/region

   United States

2. Enter your mobile phone number

   +1 [redacted] xx

   ☑ Let others find me by my phone number

3. Verify your phone

   Start

Text Messaging on Twitter

Setting up your phone allows you to:

Send tweets with text messaging on your phone.

Receive texts for DMs and the tweets from users you want to be notified about.

Clicking the phone icon on a users profile page or your followers page sets Tweet notifications for that user.

○ OFF ● ON

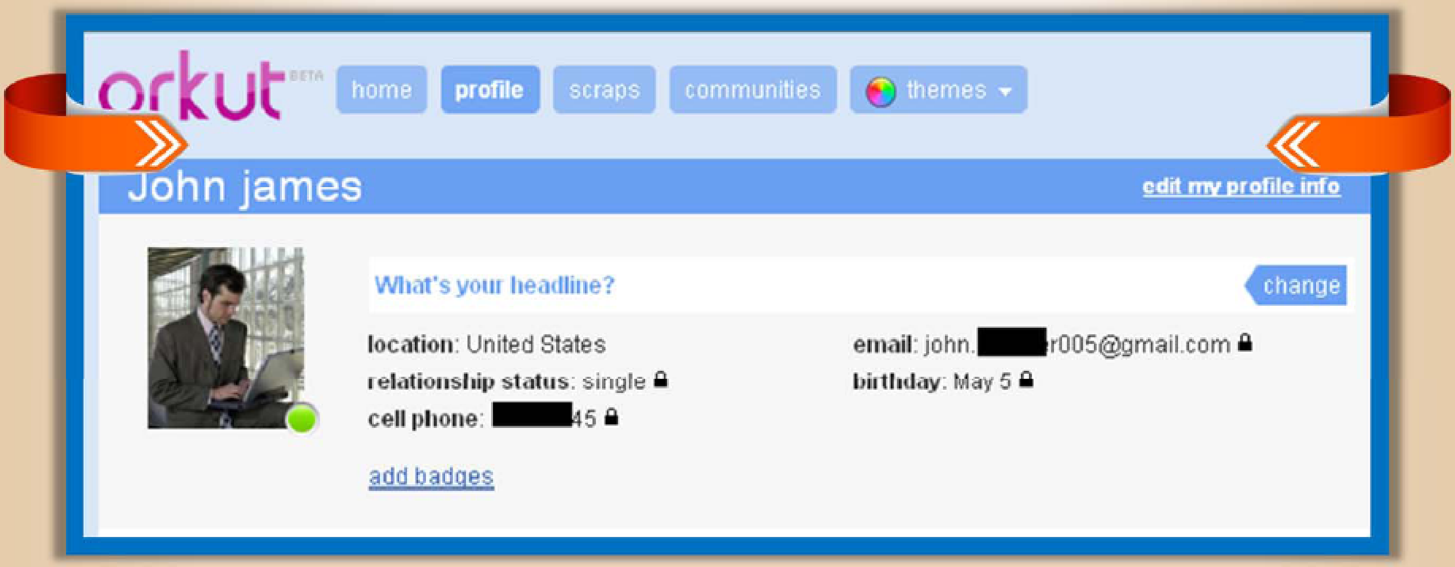
Twitter commands

Do more than Tweet! Send these commands to Twitter:

FOLLOW *username*
Start following a user

UNFOLLOW *username*
Stop following a user

Social Engineering on Orkut



John james

edit my profile info

What's your headline?

location: United States

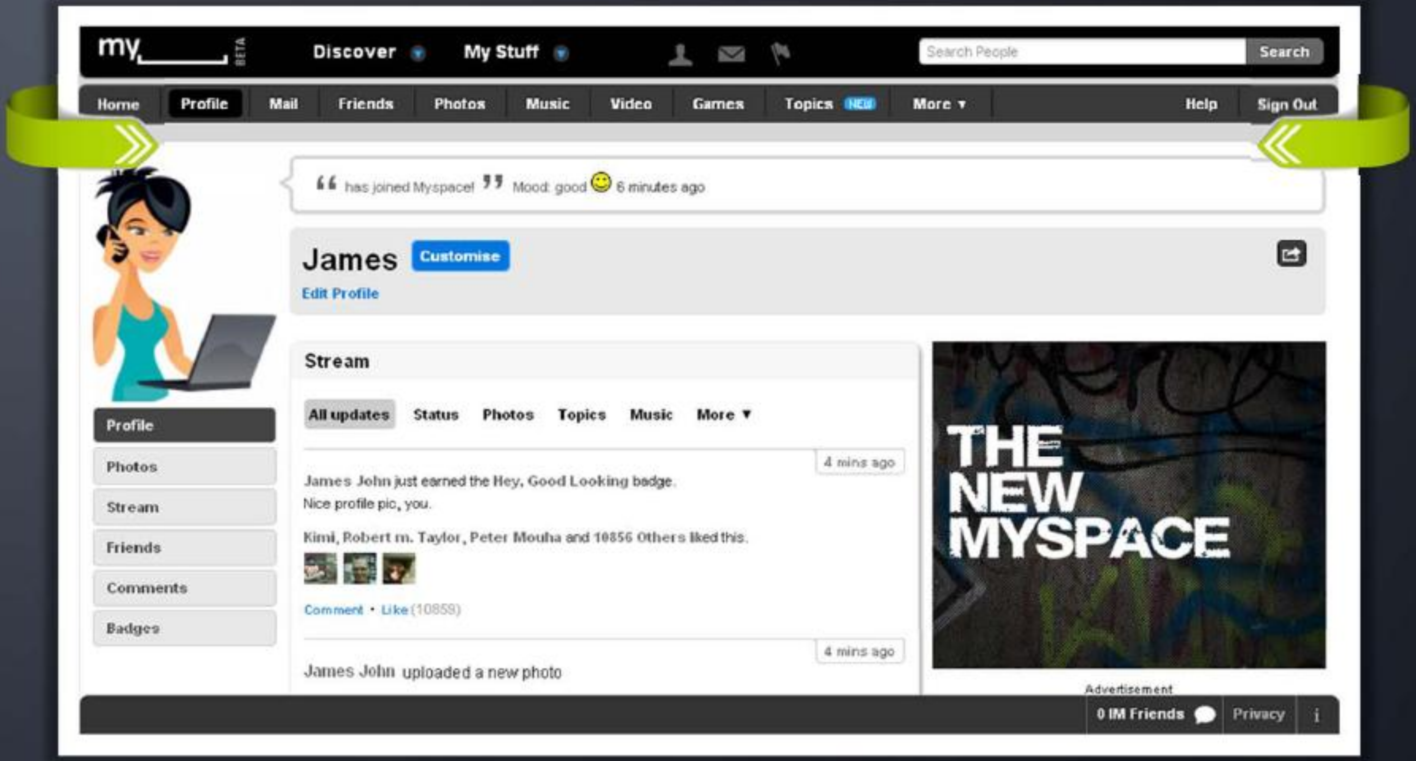
relationship status: single

cell phone: [redacted]45

email: john.[redacted]r005@gmail.com

birthday: May 5

Social Engineering on MySpace



" has joined Myspace! " Mood: good 🙂 6 minutes ago

James

4 mins ago

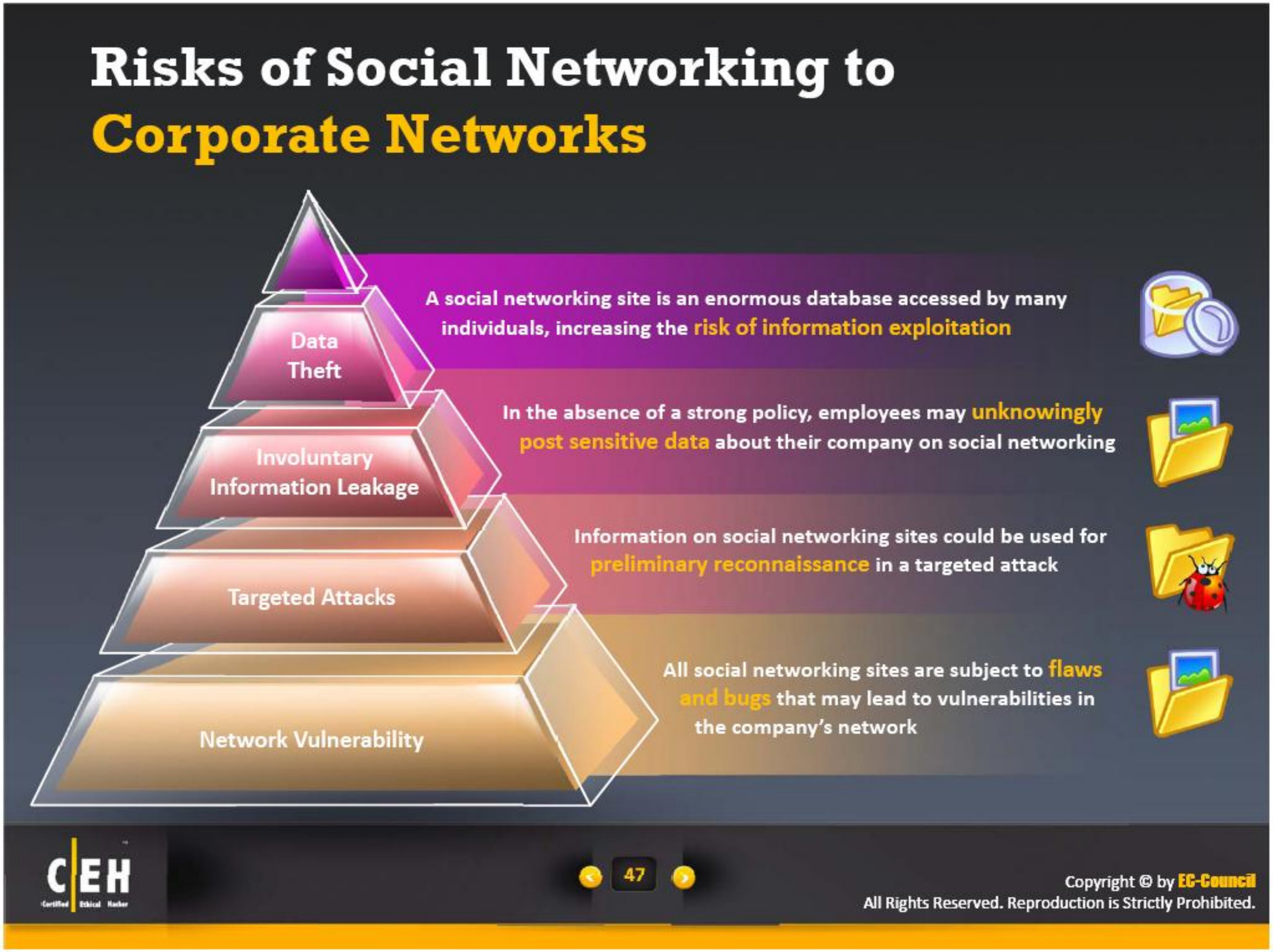
James John just earned the Hey, Good Looking badge.
Nice profile pic, you.

Kimi, Robert m. Taylor, Peter Mouha and 10856 Others liked this.

Comment • Like (10859)

4 mins ago

James John uploaded a new photo



Risks of Social Networking to Corporate Networks

Data Theft

A social networking site is an enormous database accessed by many individuals, increasing the risk of information exploitation

Involuntary Information Leakage

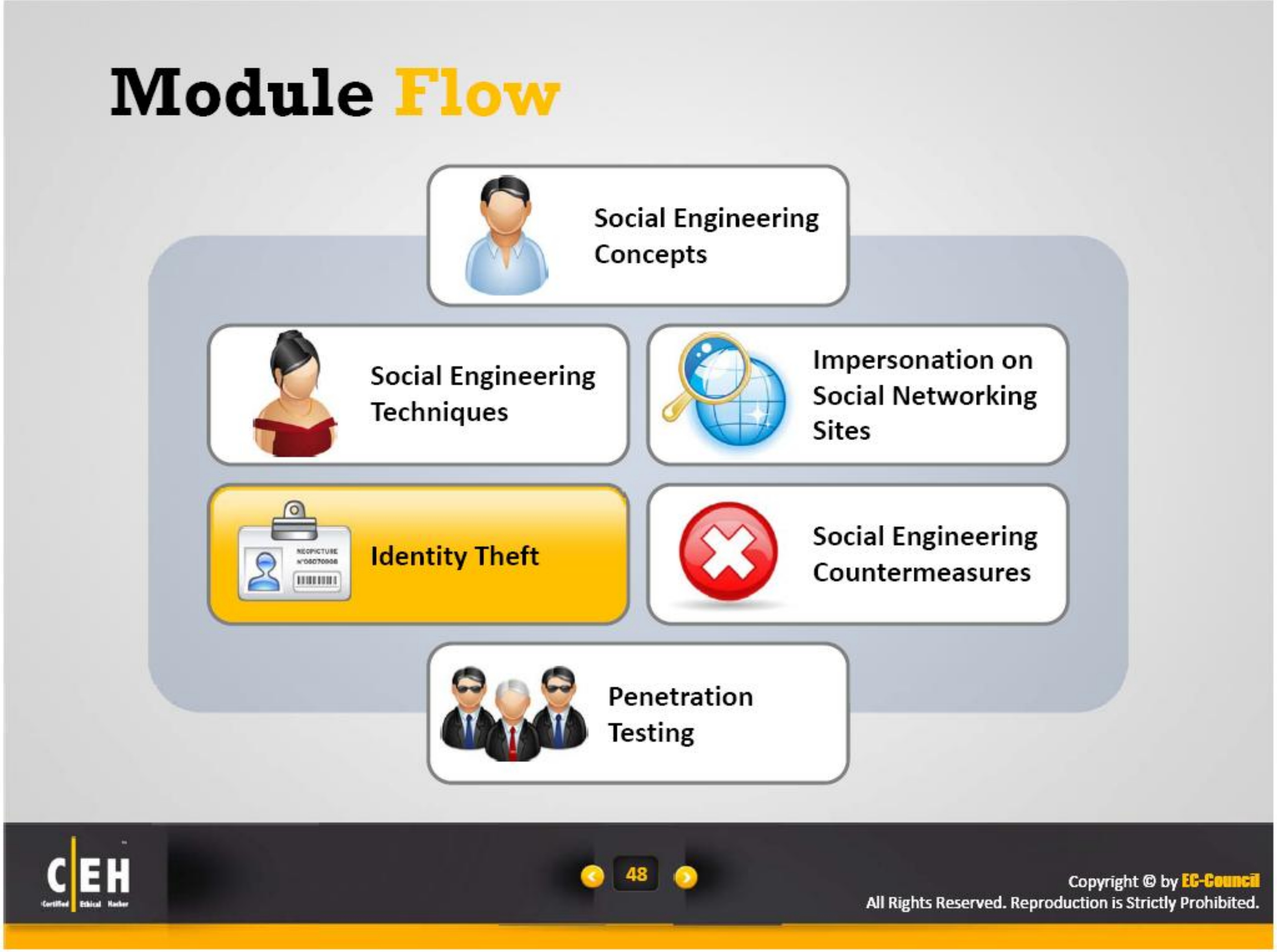
In the absence of a strong policy, employees may unknowingly post sensitive data about their company on social networking

Targeted Attacks

Information on social networking sites could be used for preliminary reconnaissance in a targeted attack

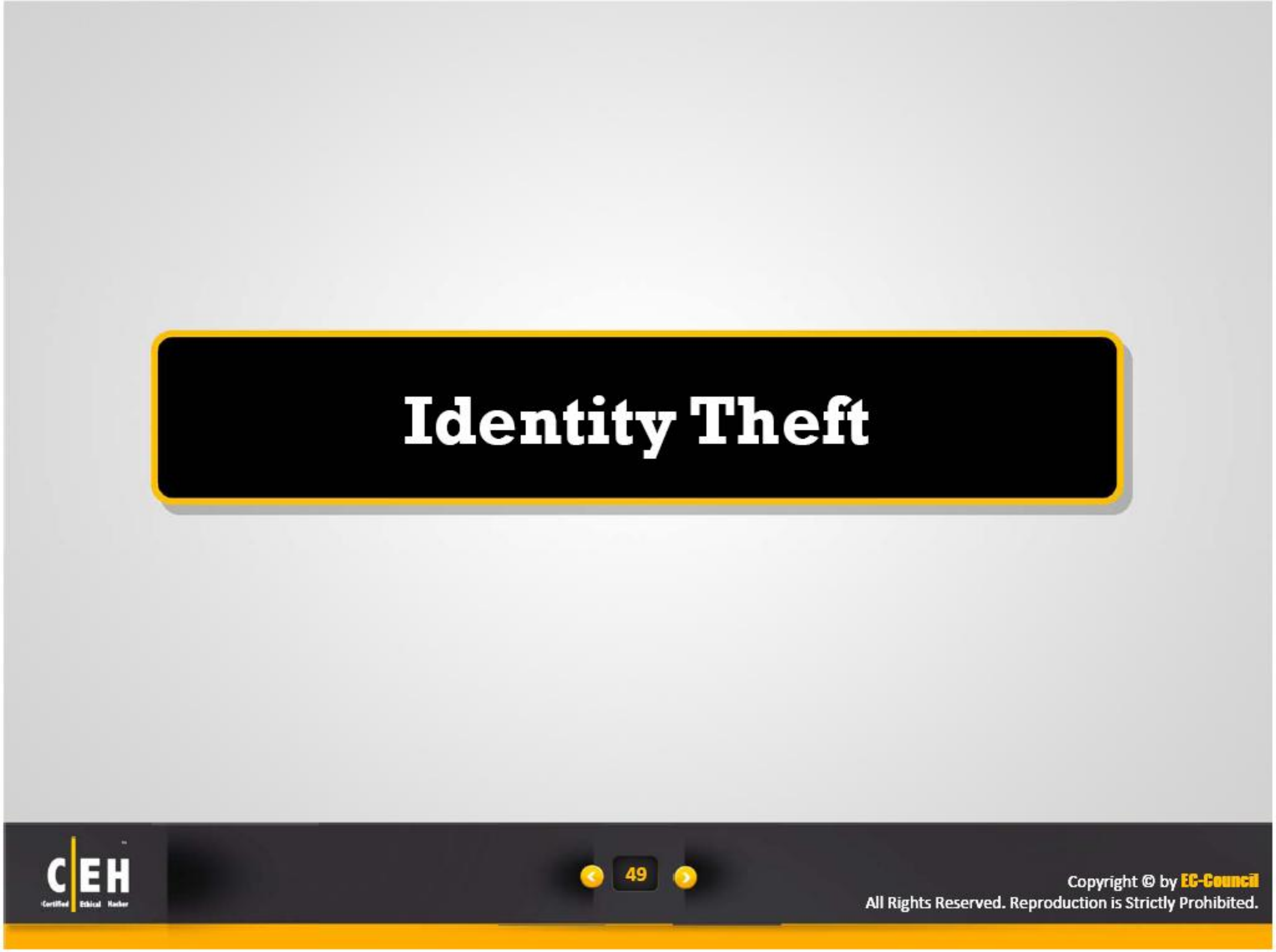
Network Vulnerability

All social networking sites are subject to flaws and bugs that may lead to vulnerabilities in the company's network

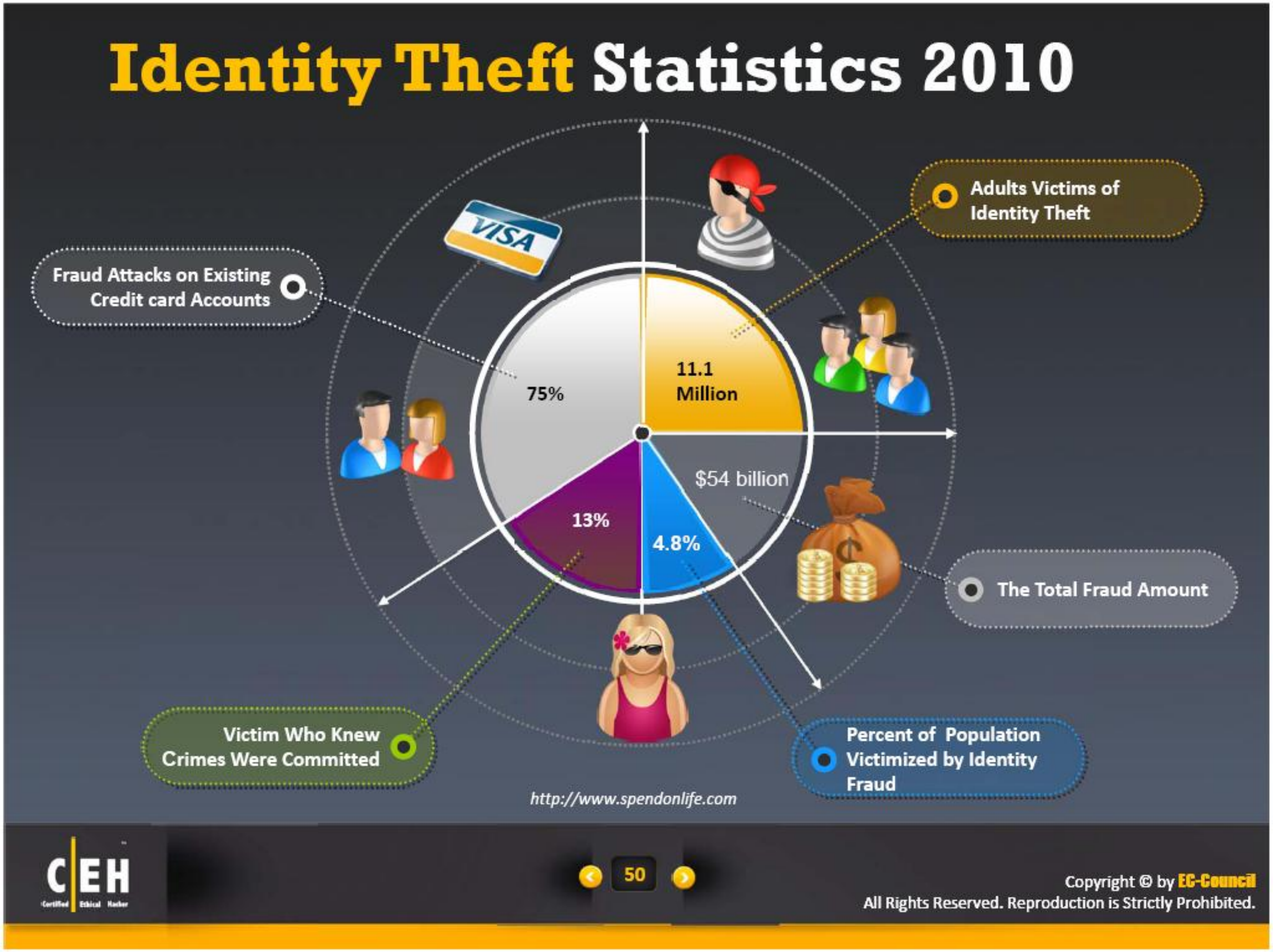


Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- **Identity Theft**
- Social Engineering Countermeasures
- Penetration Testing



Identity Theft



Identity Theft Statistics 2010

Adults Victims of Identity Theft

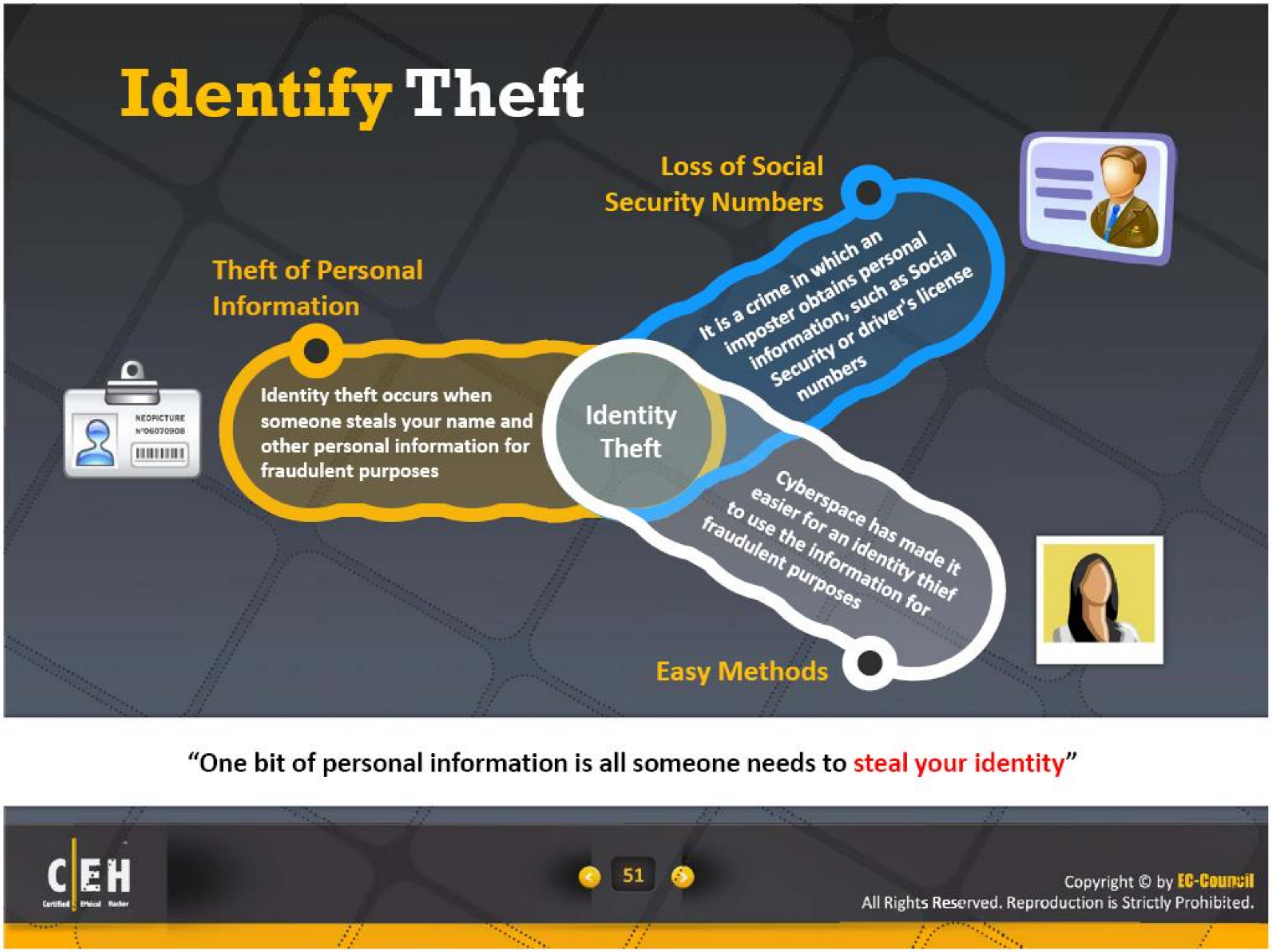
Fraud Attacks on Existing Credit card Accounts

The Total Fraud Amount

Victim Who Knew Crimes Were Committed

Percent of Population Victimized by Identity Fraud

http://www.spendonlife.com



Identify Theft

Loss of Social Security Numbers

It is a crime in which an imposter obtains personal information, such as Social Security or driver's license numbers

Theft of Personal Information

Identity theft occurs when someone steals your name and other personal information for fraudulent purposes

Identity Theft

Cyberspace has made it easier for an identity thief to use the information for fraudulent purposes

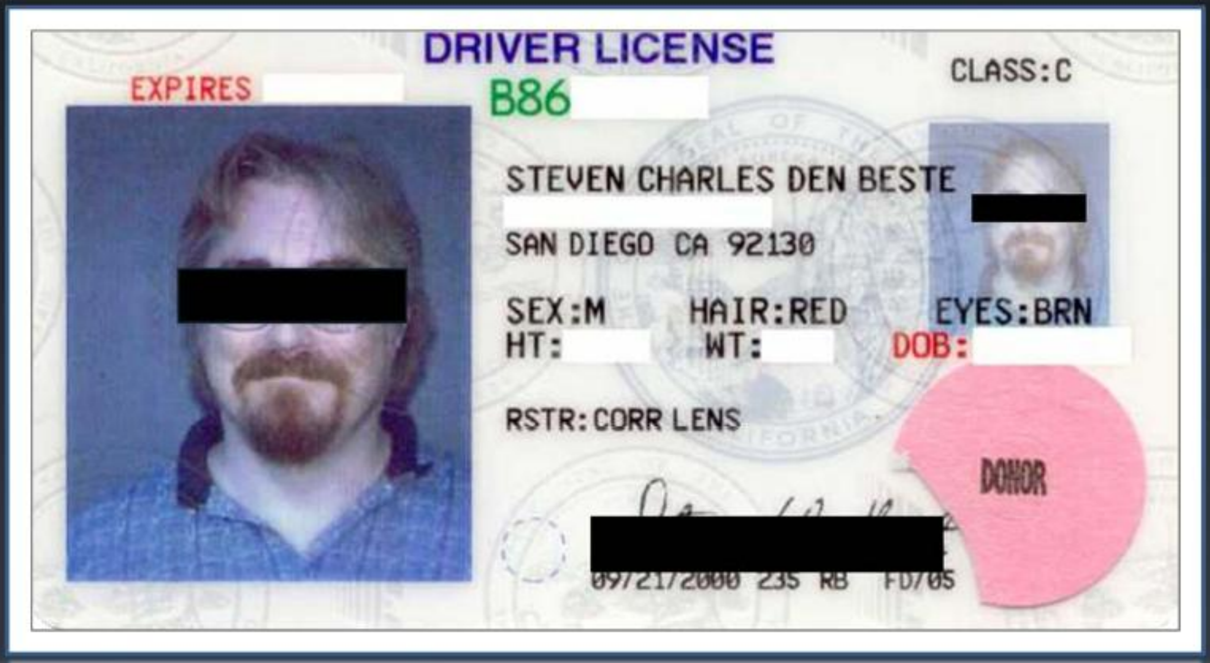
Easy Methods

"One bit of personal information is all someone needs to steal your identity"

How to Steal an Identity?

Original identity – Steven Charles

Address: San Diego CA 92130



DRIVER LICENSE

EXPIRES

B86

CLASS:C

STEVEN CHARLES DEN BESTE

SAN DIEGO CA 92130

SEX:M HAIR:RED EYES:BRN

HT: WT: DOB:

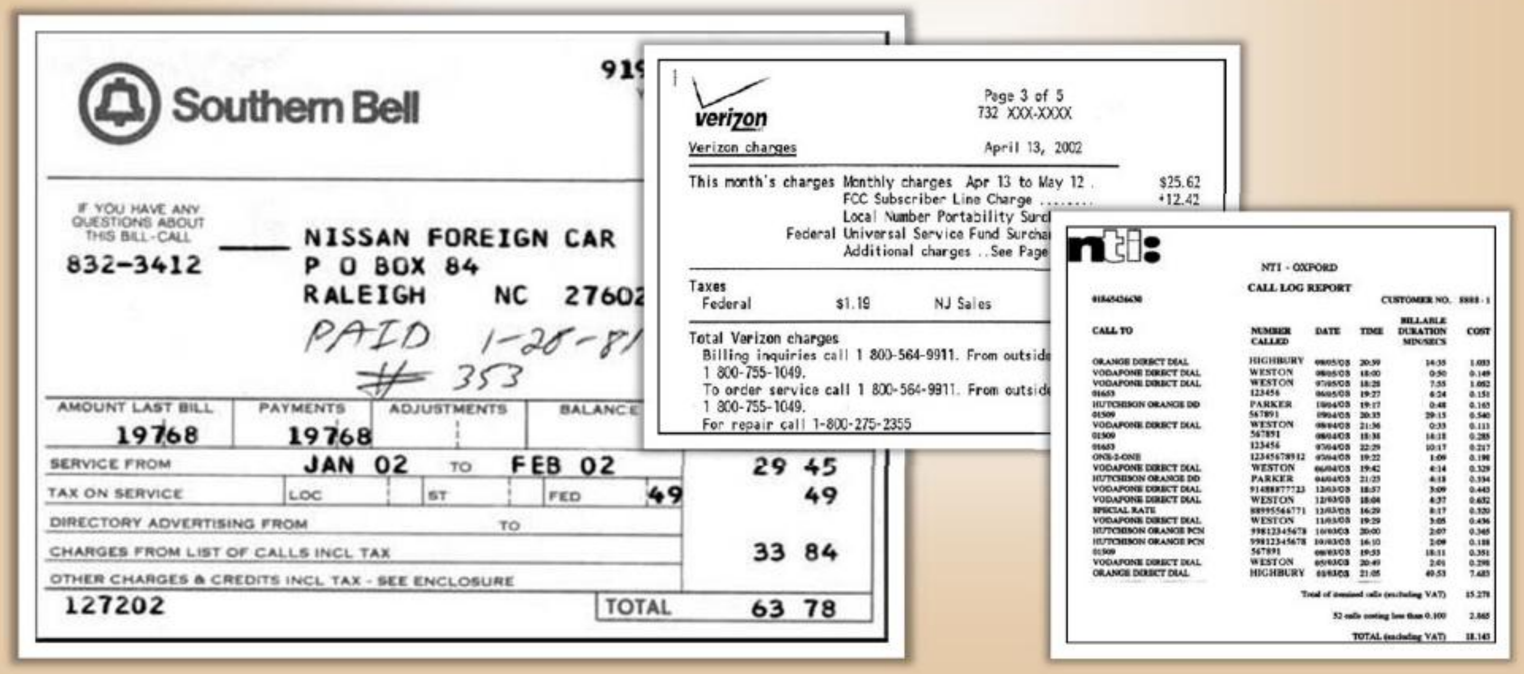
RSTR:CORR LENS

[redacted]

09/21/2000 235 RB FD/05

STEP 1

Get hold of Steven's telephone bill, water bill, or electricity bill using **dumpster diving, stolen email,** or **onsite stealing**



Southern Bell

919

IF YOU HAVE ANY QUESTIONS ABOUT THIS BILL-CALL
832-3412

NISSAN FOREIGN CAR
P O BOX 84
RALEIGH NC 27602

PAID 1-28-81
353

AMOUNT LAST BILL	PAYMENTS	ADJUSTMENTS	BALANCE
19768	19768		

SERVICE FROM	JAN 02 TO FEB 02	29 45
TAX ON SERVICE	LOC ST FED 49	49
DIRECTORY ADVERTISING FROM	TO	
CHARGES FROM LIST OF CALLS INCL TAX		33 84
OTHER CHARGES & CREDITS INCL TAX - SEE ENCLOSURE		
127202	TOTAL	63 78

verizon

Page 3 of 5
732 XXX-XXXX

Verizon charges

April 13, 2002

This month's charges Monthly charges Apr 13 to May 12 . $25.62
FCC Subscriber Line Charge .... +12.42
Local Number Portability Surc
Federal Universal Service Fund Surcha
Additional charges ..See Page

Taxes
Federal $1.19 NJ Sales

Total Verizon charges
Billing inquiries call 1 800-564-9911. From outside
1 800-755-1049.
To order service call 1 800-564-9911. From outside
1 800-755-1049.
For repair call 1-800-275-2355

nti:

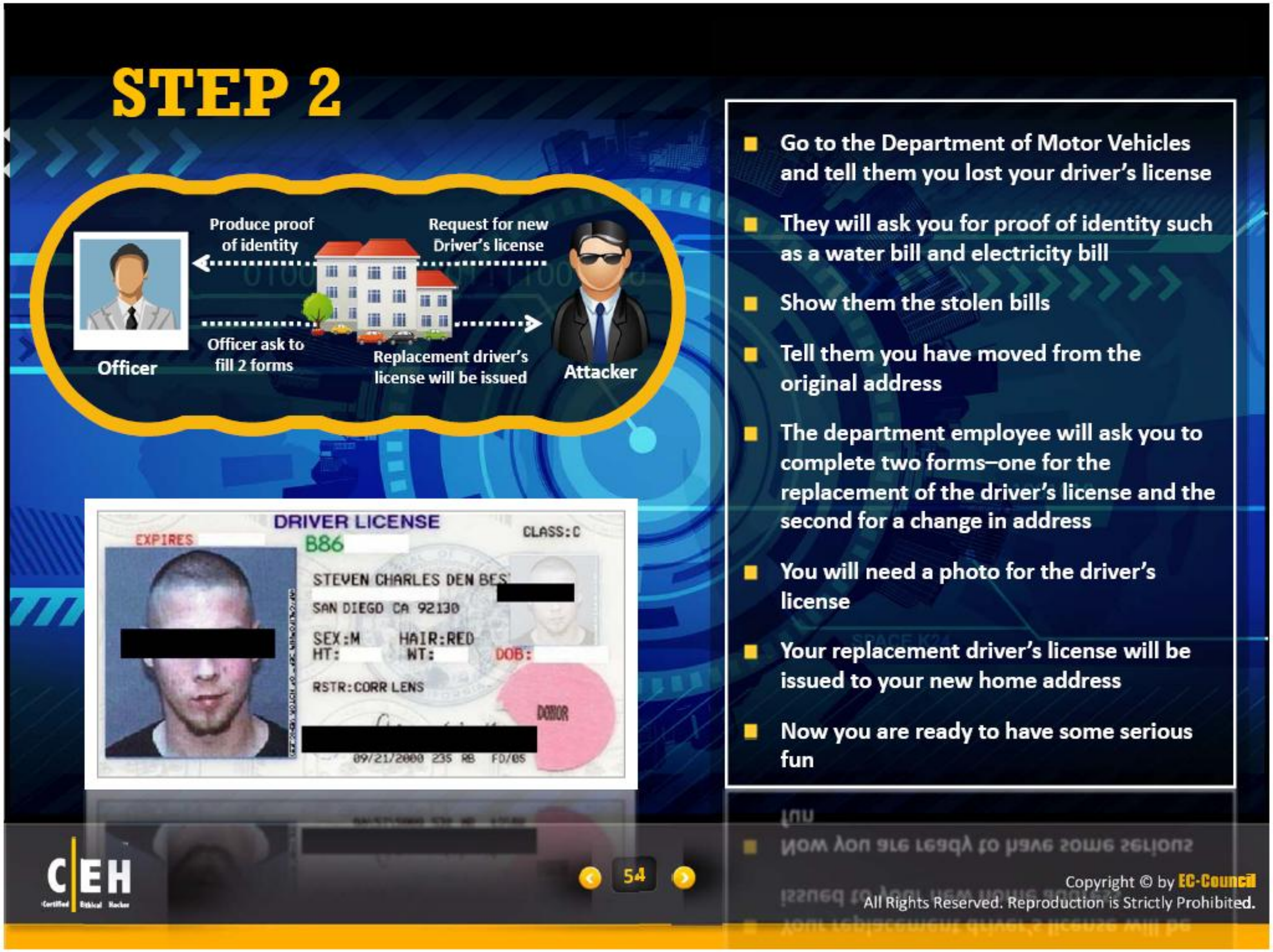
NTI - OXFORD

CALL LOG REPORT

01845426630

CUSTOMER NO. 8888 - 1

CALL TO	NUMBER CALLED	DATE	TIME	BILLABLE DURATION MIN/SECS	COST
ORANGE DIRECT DIAL	HIGHBURY	09/05/03	20:39	14:35	1.033
VODAFONE DIRECT DIAL	WESTON	08/05/03	18:00	0:50	0.149
VODAFONE DIRECT DIAL	WESTON	07/05/03	18:28	7:55	1.052
01653	123456	06/05/03	19:27	6:24	0.151
HUTCHISON ORANGE DD	PARKER	10/04/03	19:17	0:48	0.165
01509	567891	09/04/03	20:35	29:15	0.540
VODAFONE DIRECT DIAL	WESTON	09/04/03	21:36	0:33	0.111
01509	567891	08/04/03	15:38	16:15	0.285
01653	123456	07/04/03	22:29	10:17	0.217
ONE-2-ONE	123456789012	07/04/03	19:22	1:09	0.198
VODAFONE DIRECT DIAL	WESTON	06/04/03	19:42	4:14	0.329
HUTCHISON ORANGE DD	PARKER	06/04/03	21:23	4:18	0.334
VODAFONE DIRECT DIAL	91488877723	12/03/03	18:57	3:09	0.443
VODAFONE DIRECT DIAL	WESTON	12/03/03	18:04	4:37	0.632
SPECIAL RATE	88995564771	12/03/03	16:29	8:17	0.320
VODAFONE DIRECT DIAL	WESTON	11/03/03	19:29	3:05	0.436
HUTCHISON ORANGE PCN	99812345678	10/03/03	20:00	2:07	0.345
HUTCHISON ORANGE PCN	99812345678	10/03/03	16:10	2:09	0.188
01509	567891	06/03/03	19:53	18:11	0.351
VODAFONE DIRECT DIAL	WESTON	05/03/03	20:49	2:01	0.298
ORANGE DIRECT DIAL	HIGHBURY	01/03/03	21:05	49:53	7.483
				Total of itemised calls (excluding VAT)	15.278
				52 calls costing less than 0.100	2.865
				TOTAL (excluding VAT)	18.143



STEP 2

Produce proof of identity

Request for new Driver's license

Officer ask to fill 2 forms

Replacement driver's license will be issued

Officer

Attacker

DRIVER LICENSE

EXPIRES

B86

CLASS:C

[redacted]

STEVEN CHARLES DEN BES [redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED

HT: WT:

DOB:

RSTR:CORR LENS

DONOR

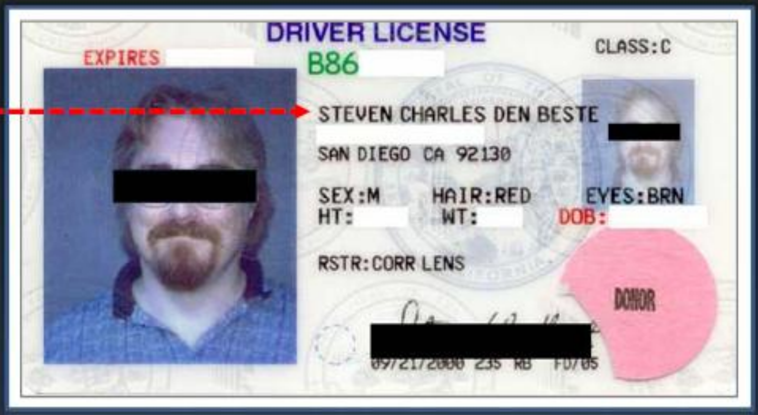
[redacted]

09/21/2000 235 RB FD/05

- Go to the Department of Motor Vehicles and tell them you lost your driver's license
- They will ask you for proof of identity such as a water bill and electricity bill
- Show them the stolen bills
- Tell them you have moved from the original address
- The department employee will ask you to complete two forms—one for the replacement of the driver's license and the second for a change in address
- You will need a photo for the driver's license
- Your replacement driver's license will be issued to your new home address
- Now you are ready to have some serious fun

Comparison

Original



DRIVER LICENSE

EXPIRES

B86

CLASS:C

STEVEN CHARLES DEN BESTE [redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED EYES:BRN

HT: WT: DOB:

RSTR:CORR LENS

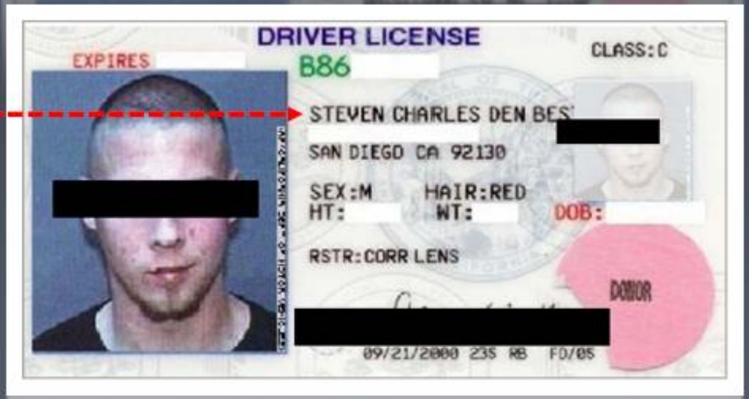
DONOR

[redacted]

09/21/2000 235 RB FD/05

Same name: Steven Charles

Identity Theft



DRIVER LICENSE

EXPIRES

B86

CLASS:C

STEVEN CHARLES DEN BES [redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED

HT: WT: DOB:

RSTR:CORR LENS

DONOR

[redacted]

09/21/2000 235 RB FD/05

STEP 3

Go to a bank in which the **original** Steven Charles has an account and tell them you would like to apply for a **new credit card**

Tell them you **do not remember** the account number and ask them to look it up using Steven's name and address

The bank will ask for your ID: Show them your **driver's license as ID**, and if the ID is accepted, your credit card will be issued and ready for use

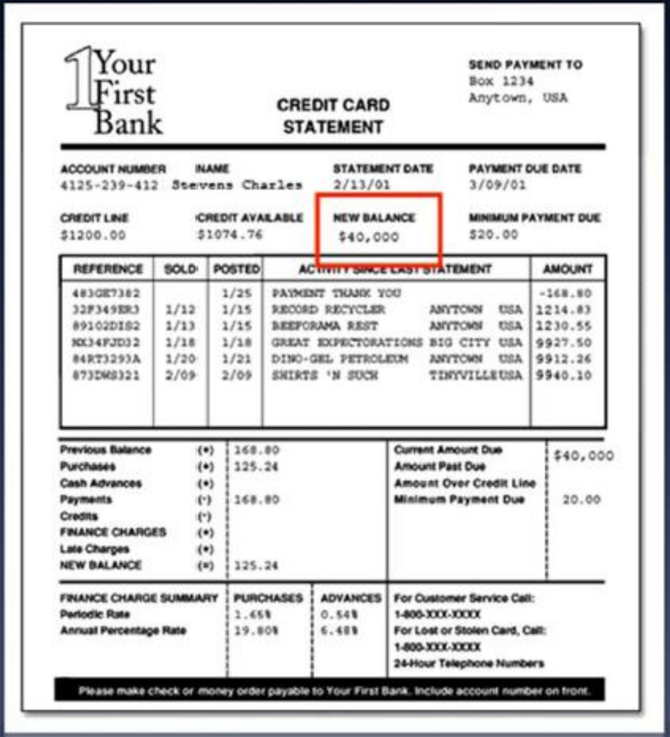
Now you are ready for shopping

Fake Steven is Ready to:

- Make purchases worth thousands of USD
- Apply for a car loan
- Apply for a new passport
- Apply for a new bank account
- Shut down your utility services

Real Steven Gets Huge Credit Card Statement

Somebody stole my identity!



Your First Bank

CREDIT CARD STATEMENT

SEND PAYMENT TO
Box 1234
Anytown, USA

ACCOUNT NUMBER	NAME	STATEMENT DATE	PAYMENT DUE DATE
4125-239-412	Stevens Charles	2/13/01	3/09/01

CREDIT LINE	CREDIT AVAILABLE	NEW BALANCE	MINIMUM PAYMENT DUE
$1200.00	$1074.76	$40,000	$20.00

REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
483GE7382		1/25	PAYMENT THANK YOU	-168.80
32F349ER3	1/12	1/15	RECORD RECYCLER ANYTOWN USA	1214.83
89102DIS2	1/13	1/15	BEEFORAMA REST ANYTOWN USA	1230.55
MK34FJD32	1/18	1/18	GREAT EXPECTORATIONS BIG CITY USA	9927.50
84RT3293A	1/20	1/21	DINO-GEL PETROLEUM ANYTOWN USA	9912.26
873DWS321	2/09	2/09	SHIRTS 'N SUCH TINYVILLEUSA	9940.10

Previous Balance	(+)	168.80	Current Amount Due	$40,000
Purchases	(+)	125.24	Amount Past Due	
Cash Advances	(+)		Amount Over Credit Line	
Payments	(-)	168.80	Minimum Payment Due	20.00
Credits	(-)			
FINANCE CHARGES	(+)			
Late Charges	(+)			
NEW BALANCE	(=)	125.24		

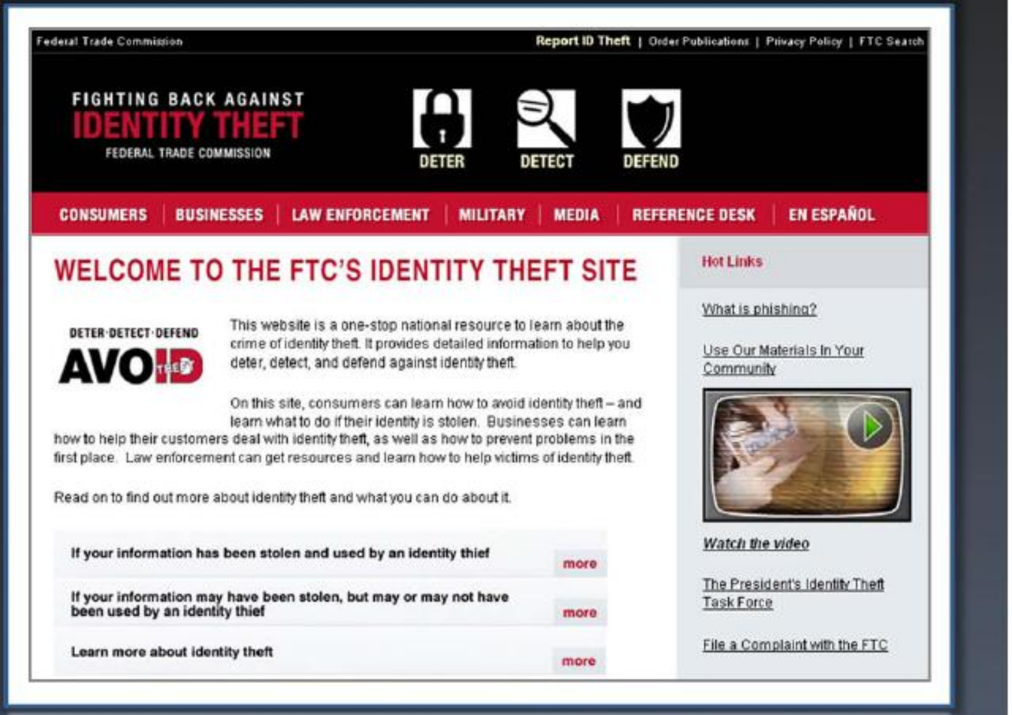
FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES
Periodic Rate	1.65%	0.54%
Annual Percentage Rate	19.80%	6.48%

For Customer Service Call:
1-800-XXX-XXXX
For Lost or Stolen Card, Call:
1-800-XXX-XXXX
24-Hour Telephone Numbers

Please make check or money order payable to Your First Bank. Include account number on front.

Identity Theft - Serious Problem

- Identity theft is a serious problem
- The number of violations has increased
- Securing personal information in the workplace and at home and looking over credit card reports are just a few of the ways to minimize the risk of identity theft



Federal Trade Commission | **Report ID Theft** | Order Publications | Privacy Policy | FTC Search

FIGHTING BACK AGAINST **IDENTITY THEFT** FEDERAL TRADE COMMISSION

DETER | DETECT | DEFEND

CONSUMERS | BUSINESSES | LAW ENFORCEMENT | MILITARY | MEDIA | REFERENCE DESK | EN ESPAÑOL

WELCOME TO THE FTC'S IDENTITY THEFT SITE

DETER·DETECT·DEFEND AVOID THEFT

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

On this site, consumers can learn how to avoid identity theft – and learn what to do if their identity is stolen. Businesses can learn how to help their customers deal with identity theft, as well as how to prevent problems in the first place. Law enforcement can get resources and learn how to help victims of identity theft.

Read on to find out more about identity theft and what you can do about it.

If your information has been stolen and used by an identity thief more

If your information may have been stolen, but may or may not have been used by an identity thief more

Learn more about identity theft more

Hot Links

What is phishing?

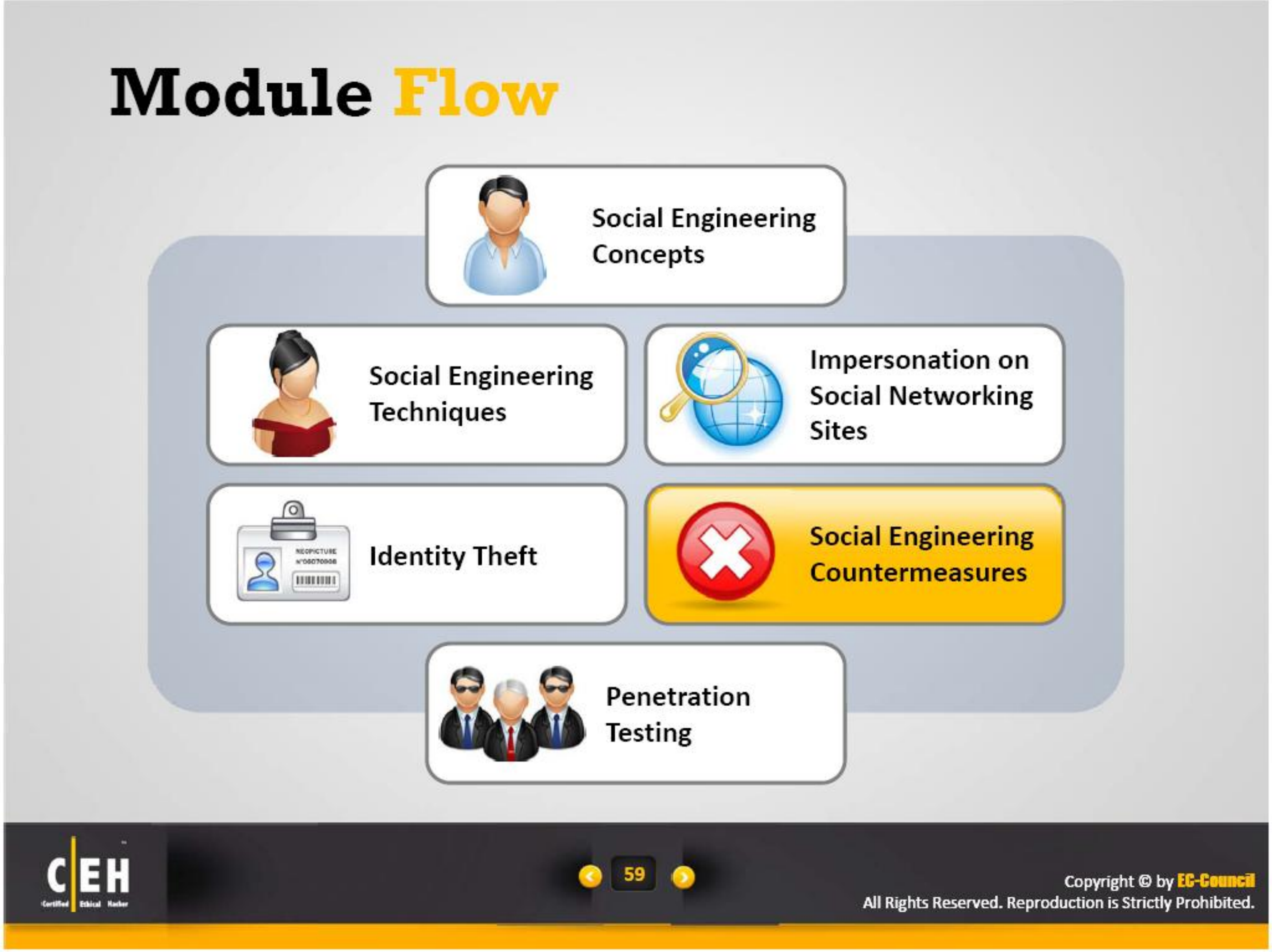
Use Our Materials In Your Community

Watch the video

The President's Identity Theft Task Force

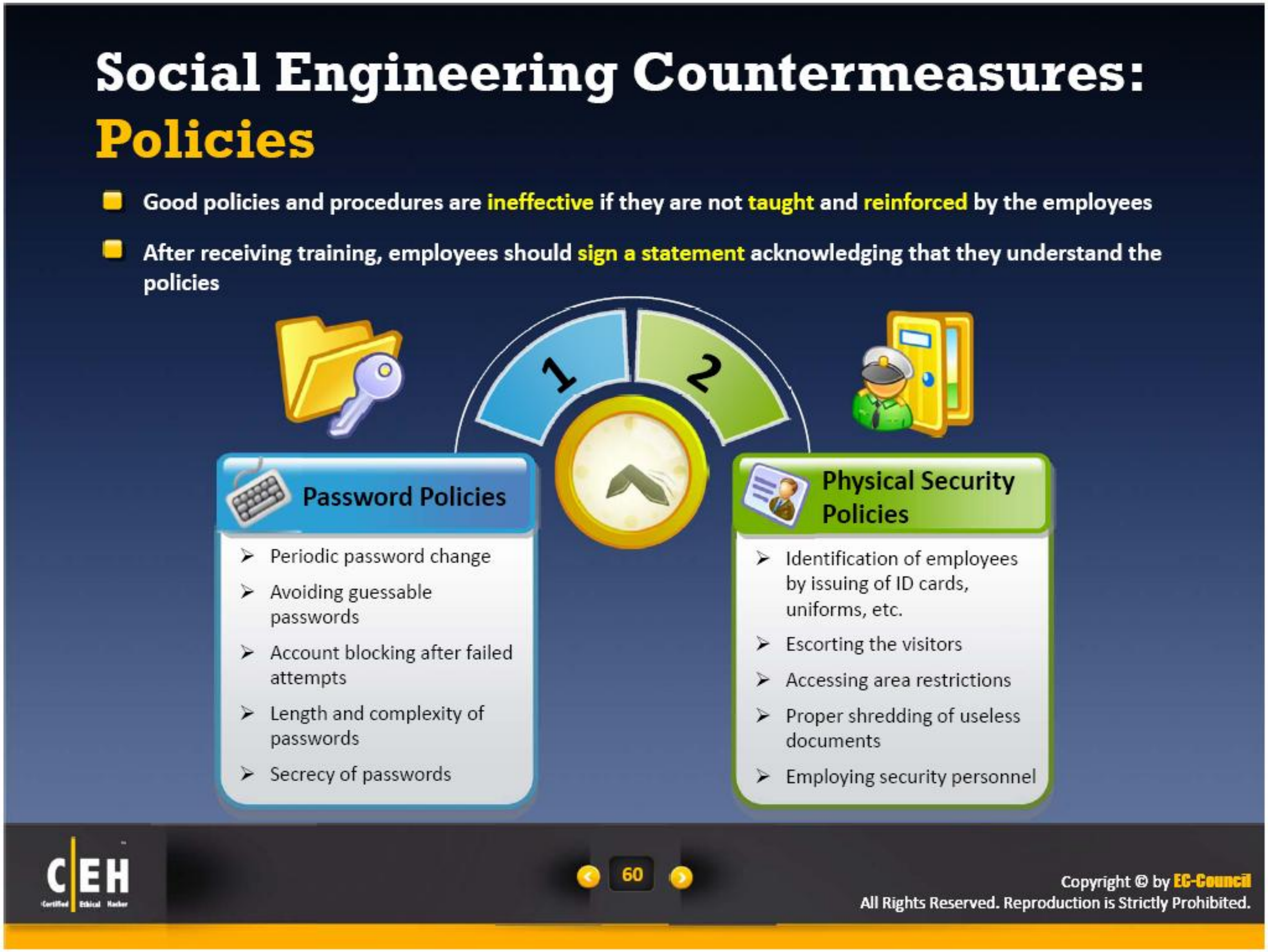
File a Complaint with the FTC

http://www.consumer.gov



Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing



Social Engineering Countermeasures: Policies

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies

1

2

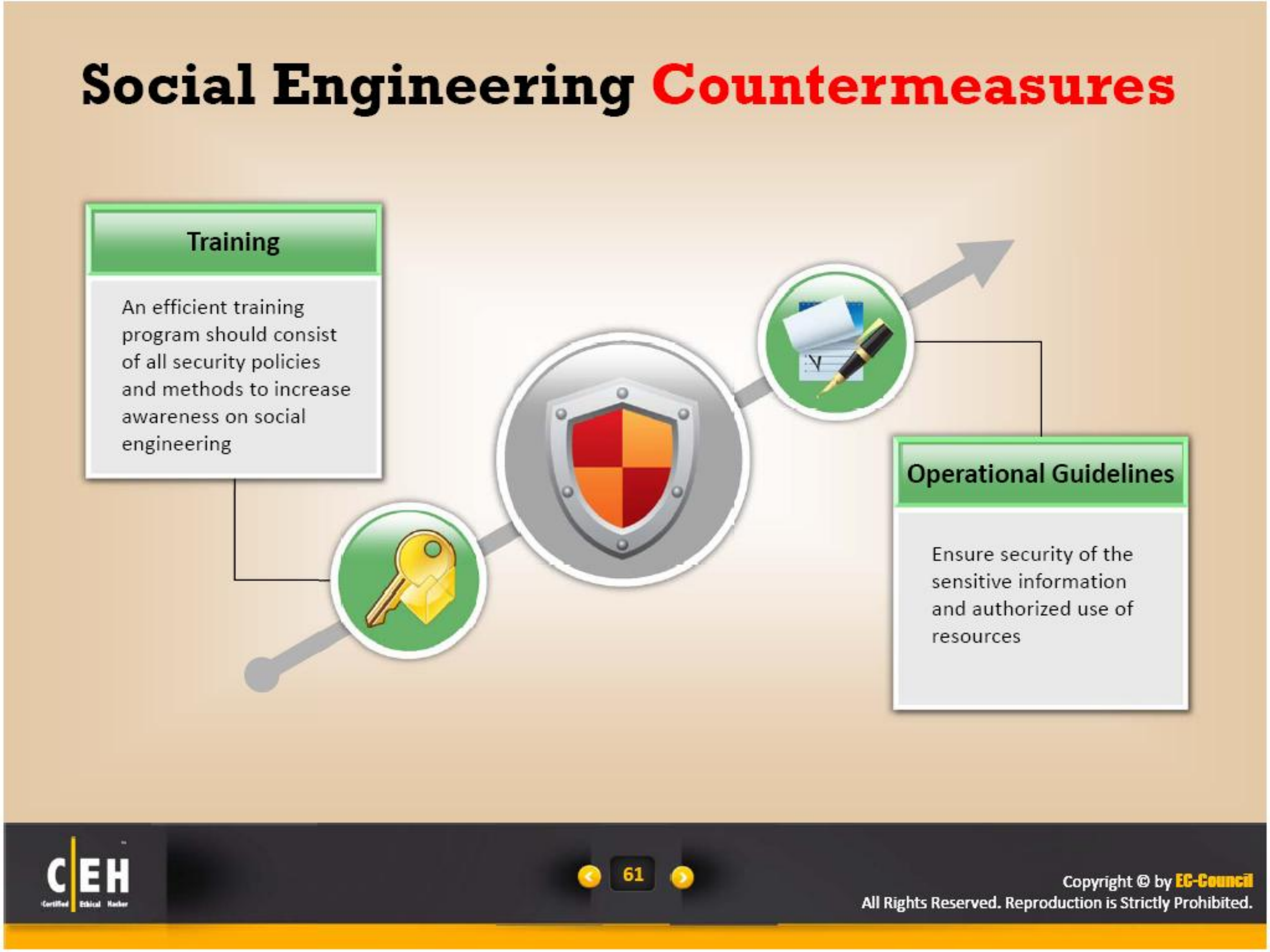
Password Policies

- Periodic password change
- Avoiding guessable passwords
- Account blocking after failed attempts
- Length and complexity of passwords
- Secrecy of passwords

Physical Security Policies

- Identification of employees by issuing of ID cards, uniforms, etc.
- Escorting the visitors
- Accessing area restrictions
- Proper shredding of useless documents
- Employing security personnel

60



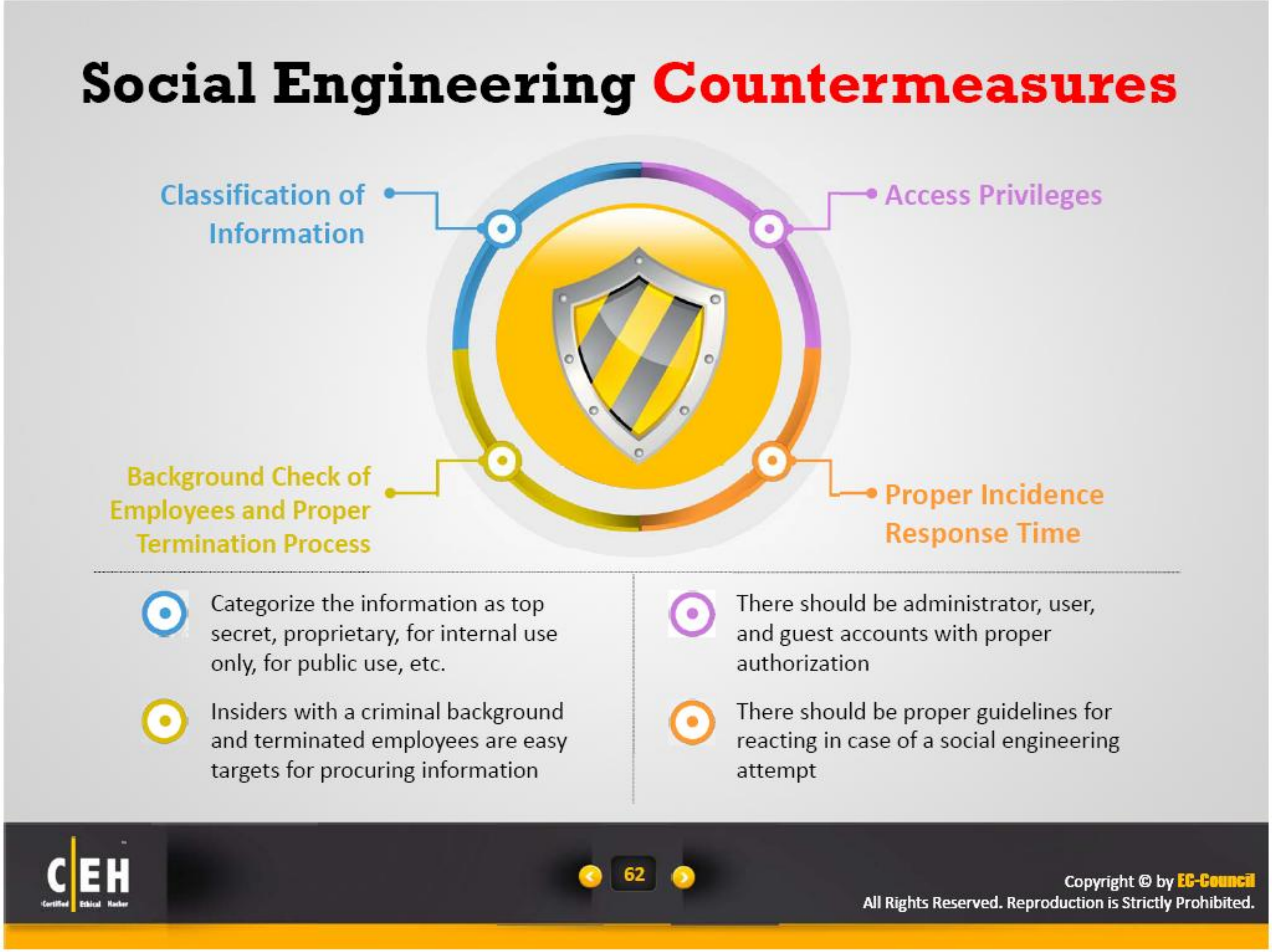
Social Engineering Countermeasures

Training

An efficient training program should consist of all security policies and methods to increase awareness on social engineering

Operational Guidelines

Ensure security of the sensitive information and authorized use of resources



Social Engineering Countermeasures

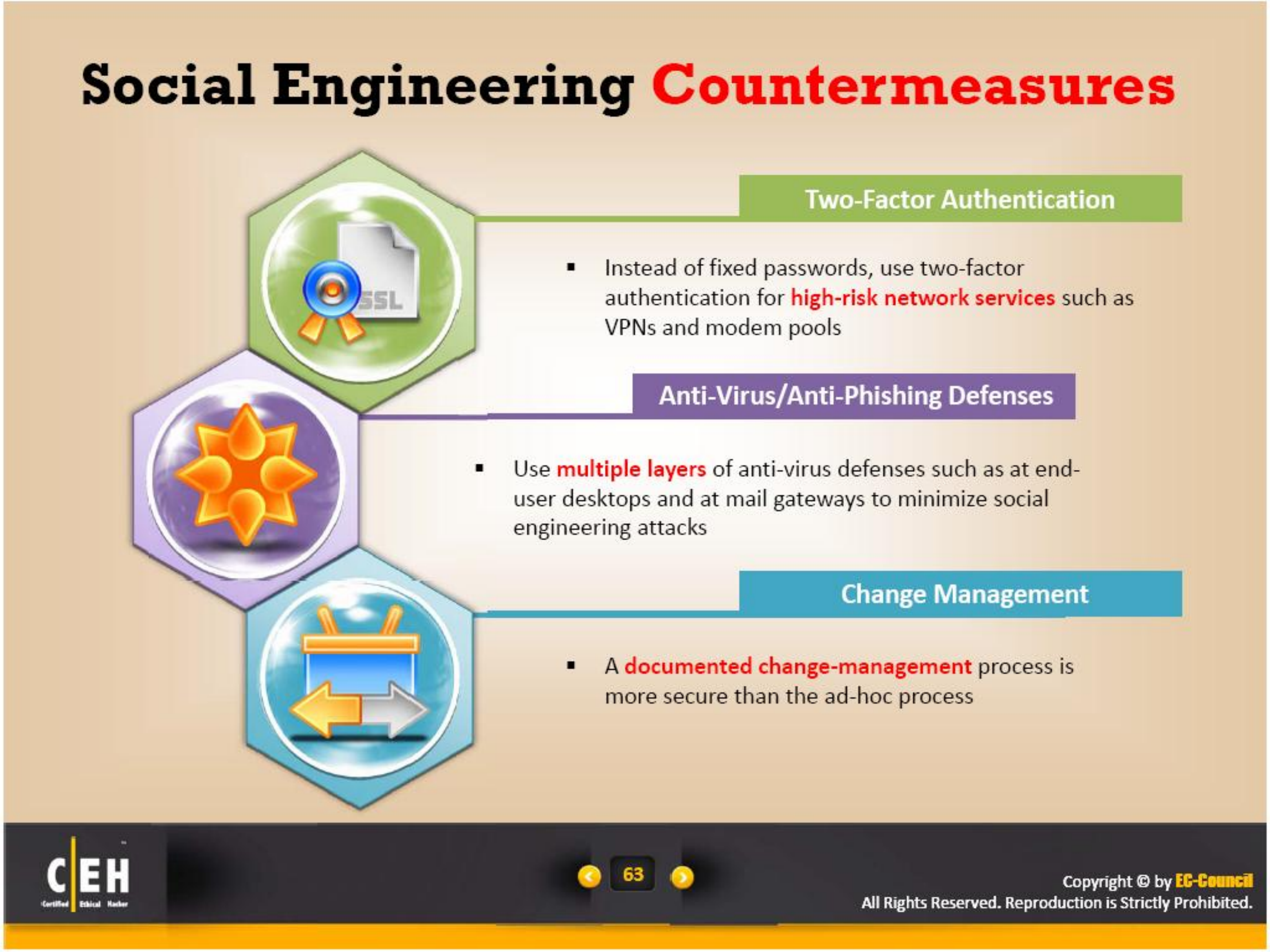
Classification of Information

Access Privileges

Background Check of Employees and Proper Termination Process

Proper Incidence Response Time

- Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
- Insiders with a criminal background and terminated employees are easy targets for procuring information
- There should be administrator, user, and guest accounts with proper authorization
- There should be proper guidelines for reacting in case of a social engineering attempt



Social Engineering Countermeasures

Two-Factor Authentication

- Instead of fixed passwords, use two-factor authentication for **high-risk network services** such as VPNs and modem pools

Anti-Virus/Anti-Phishing Defenses

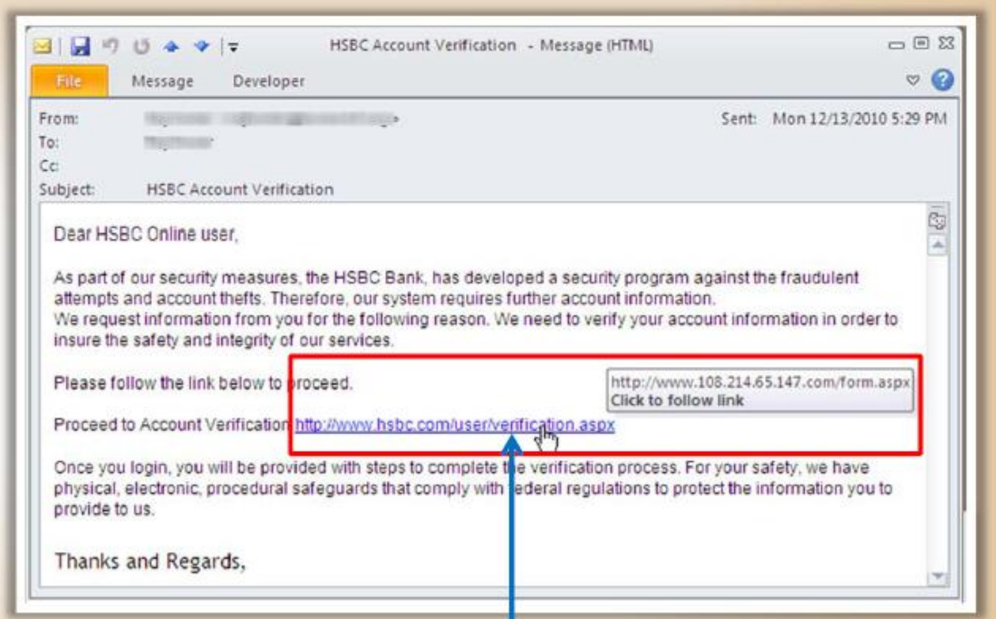
- Use **multiple layers** of anti-virus defenses such as at end-user desktops and at mail gateways to minimize social engineering attacks

Change Management

- A **documented change-management** process is more secure than the ad-hoc process

How to Detect Phishing Emails?

- It includes links that **lead to spoofed websites** asking to enter personal information when clicked
- The phishing email seems to be **from a bank, financial institution**, company, or social networking site
- Seems to be from a person who is **listed in your email address book**
- Directs to **call a phone number** in order to give up account number, personal identification number, password, or confidential information
- Includes **official-looking logos and other information** taken directly from legitimate websites convincing you to disclose your personal details



From: [redacted]

To: [redacted]

Cc:

Subject: HSBC Account Verification

Sent: Mon 12/13/2010 5:29 PM

Dear HSBC Online user,

As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information.
We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

Please follow the link below to proceed.

Proceed to Account Verification http://www.hsbc.com/user/verification.aspx

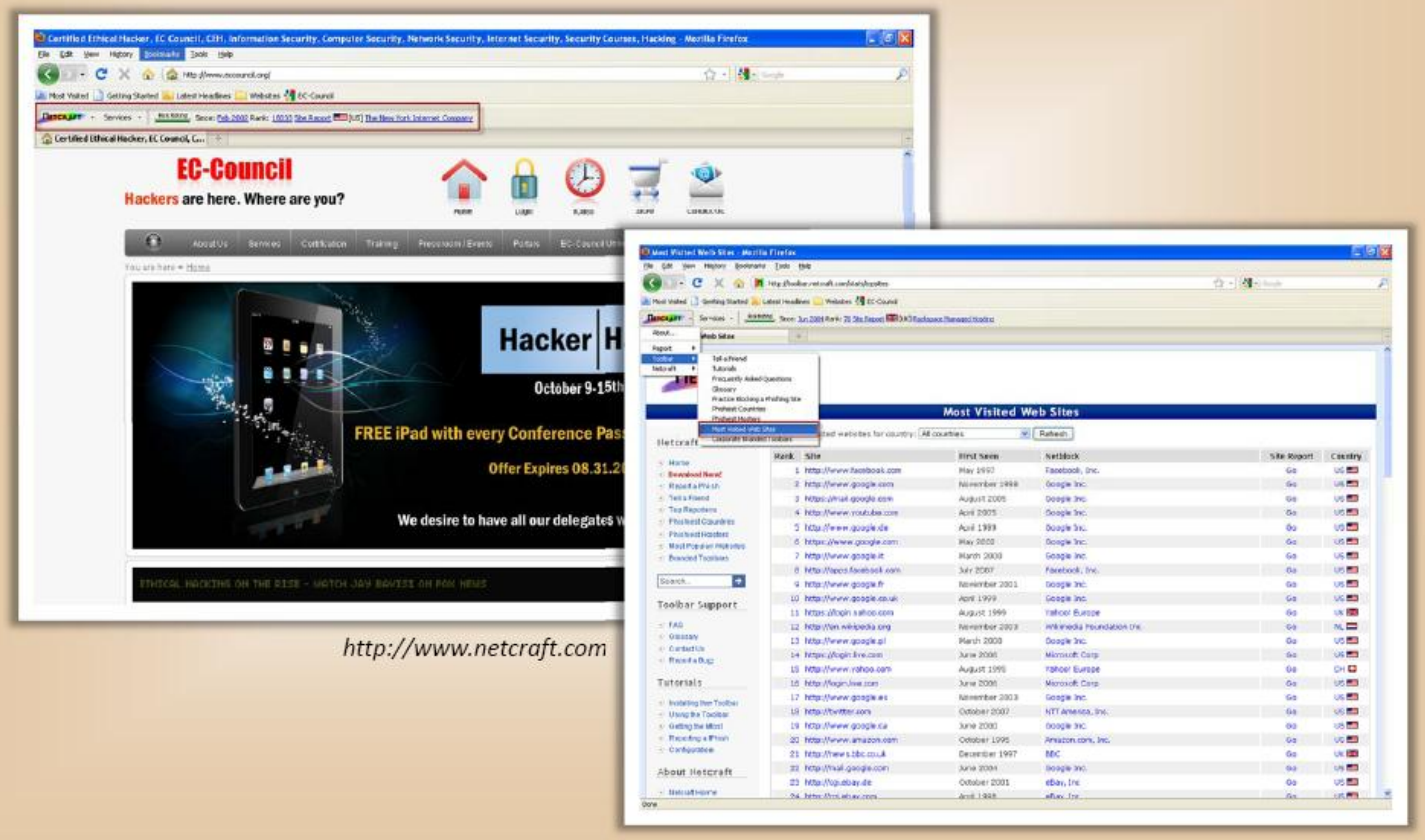
http://www.108.214.65.147.com/form.aspx
Click to follow link

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.

Thanks and Regards,

Link that seems to be legitimate but leads to **spoofed** website

Anti-Phishing Toolbar: Netcraft


Certified Ethical Hacker, EC Council, CEH, Information Security, Computer Security, Network Security, Internet Security, Security Courses, Hacking - Mozilla Firefox
EC-Council
Hackers are here. Where are you?
Hacker H
October 9-15th
FREE iPad with every Conference Pas
Offer Expires 08.31.2
We desire to have all our delegates w
Most Visited Web Sites - Mozilla Firefox
Netcraft
Toolbar Support
Tutorials
About Netcraft

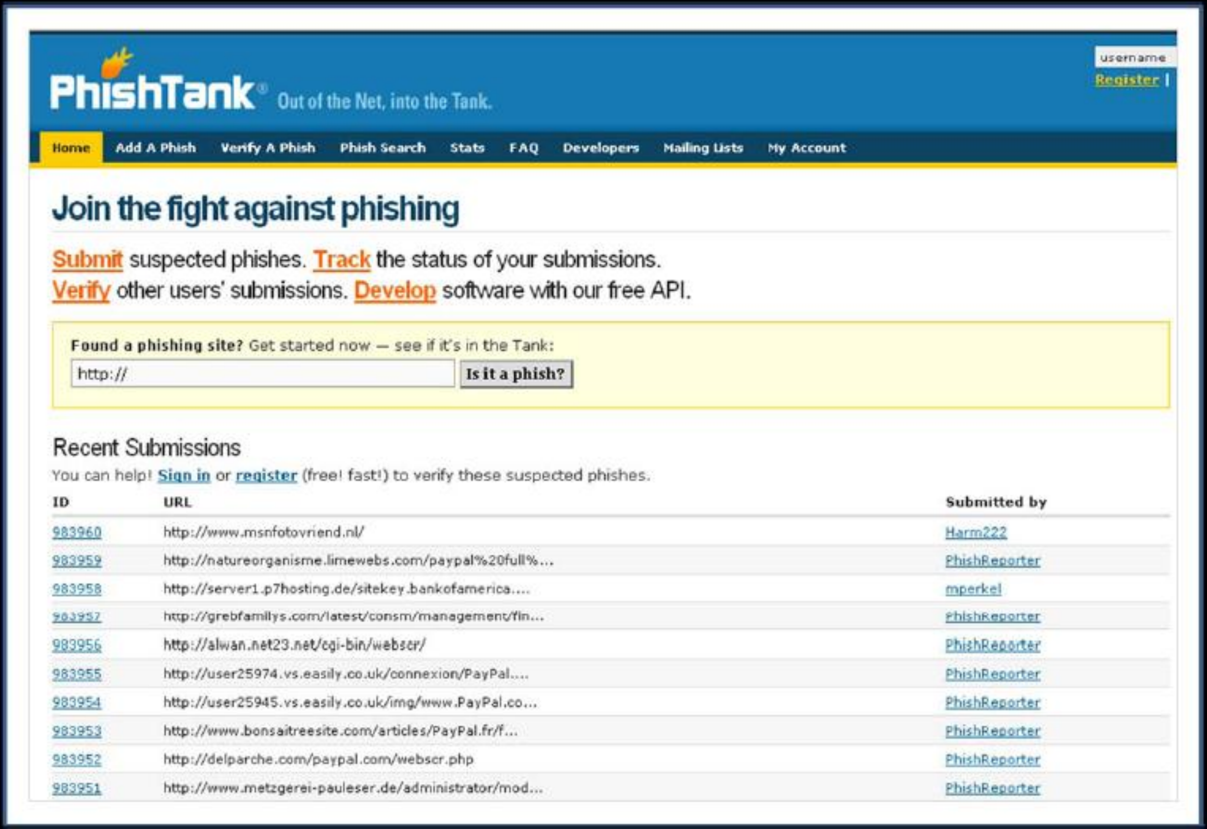
Most Visited Web Sites

ted websites for country: All countries Refresh

Rank	Site	First Seen	Netblock	Site Report	Country
1	http://www.facebook.com	May 1997	Facebook, Inc.	Go	US
2	http://www.google.com	November 1998	Google Inc.	Go	US
3	https://mail.google.com	August 2005	Google Inc.	Go	US
4	http://www.youtube.com	April 2005	Google Inc.	Go	US
5	http://www.google.de	April 1999	Google Inc.	Go	US
6	https://www.google.com	May 2002	Google Inc.	Go	US
7	http://www.google.it	March 2000	Google Inc.	Go	US
8	http://apps.facebook.com	July 2007	Facebook, Inc.	Go	US
9	http://www.google.fr	November 2001	Google Inc.	Go	US
10	http://www.google.co.uk	April 1999	Google Inc.	Go	US
11	https://login.yahoo.com	August 1999	Yahoo! Europe	Go	UK
12	http://en.wikipedia.org	November 2003	Wikimedia Foundation Inc.	Go	NL
13	http://www.google.pl	March 2000	Google Inc.	Go	US
14	https://login.live.com	June 2006	Microsoft Corp	Go	US
15	http://www.yahoo.com	August 1995	Yahoo! Europe	Go	CH
16	http://login.live.com	June 2006	Microsoft Corp	Go	US
17	http://www.google.es	November 2003	Google Inc.	Go	US
18	http://twitter.com	October 2007	NTT America, Inc.	Go	US
19	http://www.google.ca	June 2000	Google Inc.	Go	US
20	http://www.amazon.com	October 1995	Amazon.com, Inc.	Go	US
21	http://news.bbc.co.uk	December 1997	BBC	Go	UK
22	http://mail.google.com	June 2004	Google Inc.	Go	US
23	http://cgi.ebay.de	October 2001	eBay, Inc	Go	US
24	http://cgi.ebay.com	April 1998	eBay, Inc	Go	US

http://www.netcraft.com

Anti-Phishing Toolbar: PhishTank



Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

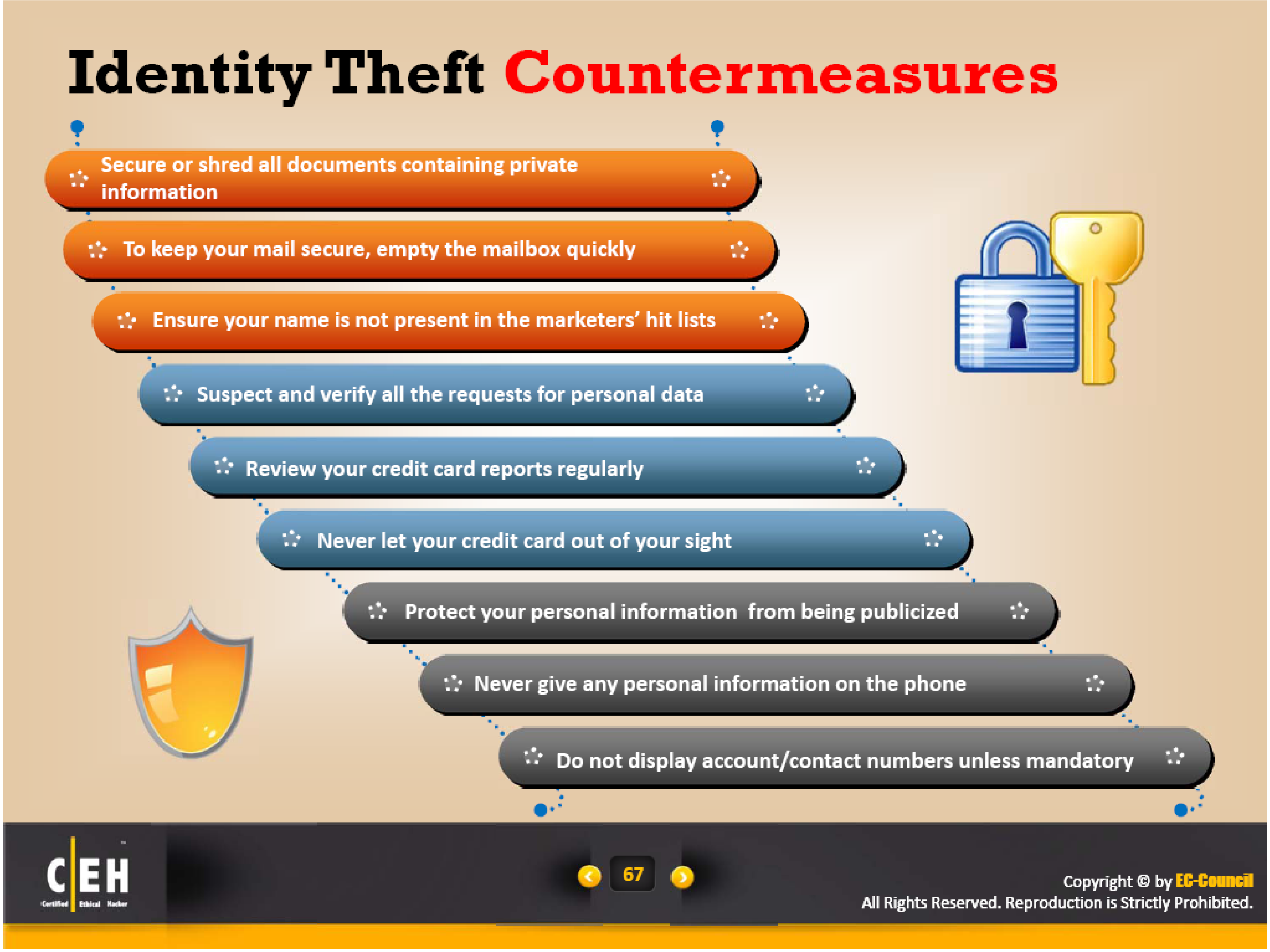
http:// [Is it a phish?]

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

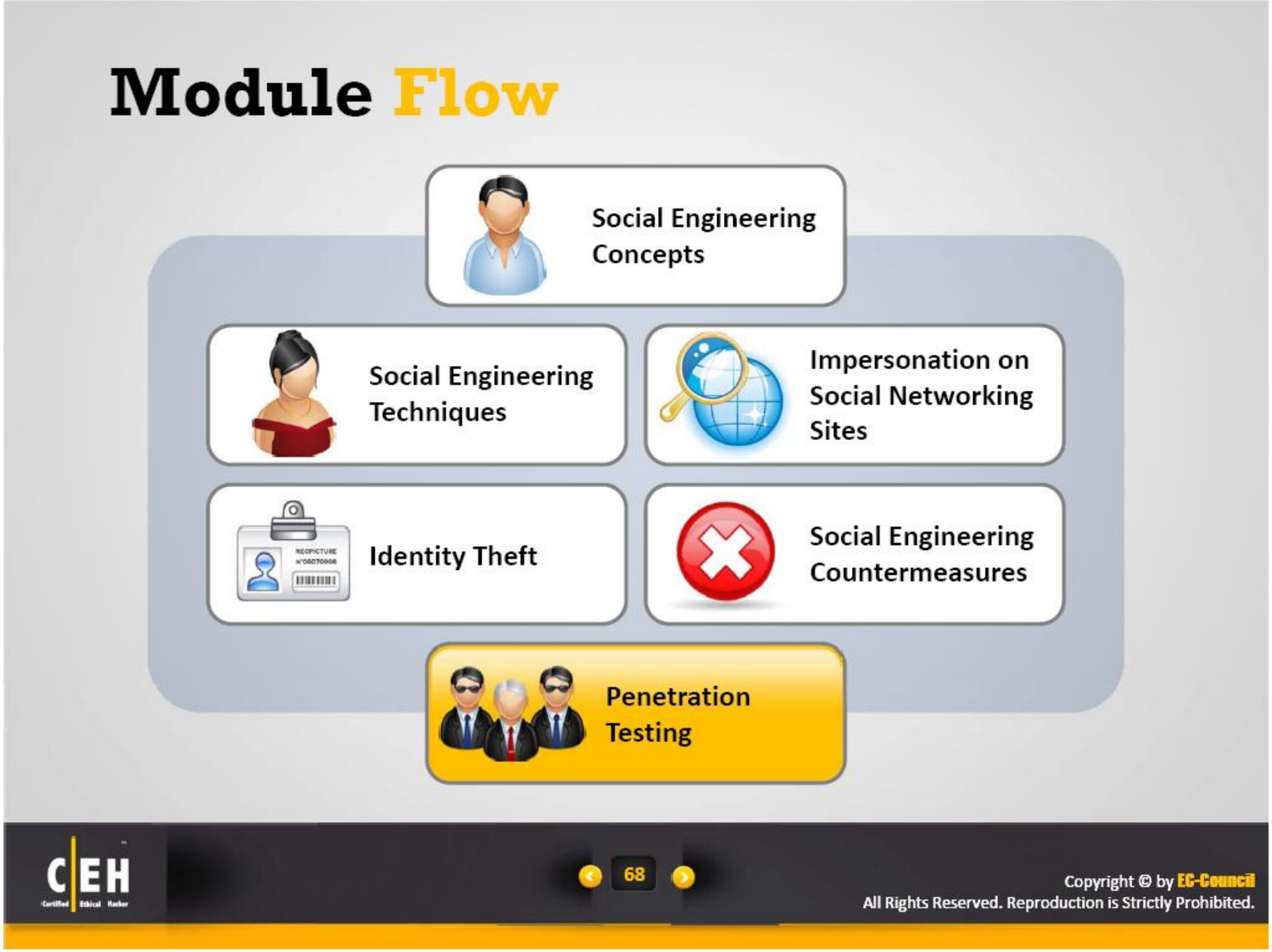
ID	URL	Submitted by
983960	http://www.msnfotovriend.nl/	Harm222
983959	http://natureorganisme.limewebs.com/paypal%20full%...	PhishReporter
983958	http://server1.p7hosting.de/sitekey.bankofamerica....	mperkel
983957	http://grebfamilys.com/latest/consm/management/fin...	PhishReporter
983956	http://alwan.net23.net/cgi-bin/webscr/	PhishReporter
983955	http://user25974.vs.easily.co.uk/connexion/PayPal....	PhishReporter
983954	http://user25945.vs.easily.co.uk/img/www.PayPal.co...	PhishReporter
983953	http://www.bonsaitreesite.com/articles/PayPal.fr/f...	PhishReporter
983952	http://delparche.com/paypal.com/webscr.php	PhishReporter
983951	http://www.metzgerei-pauleser.de/administrator/mod...	PhishReporter

http://www.phishtank.com



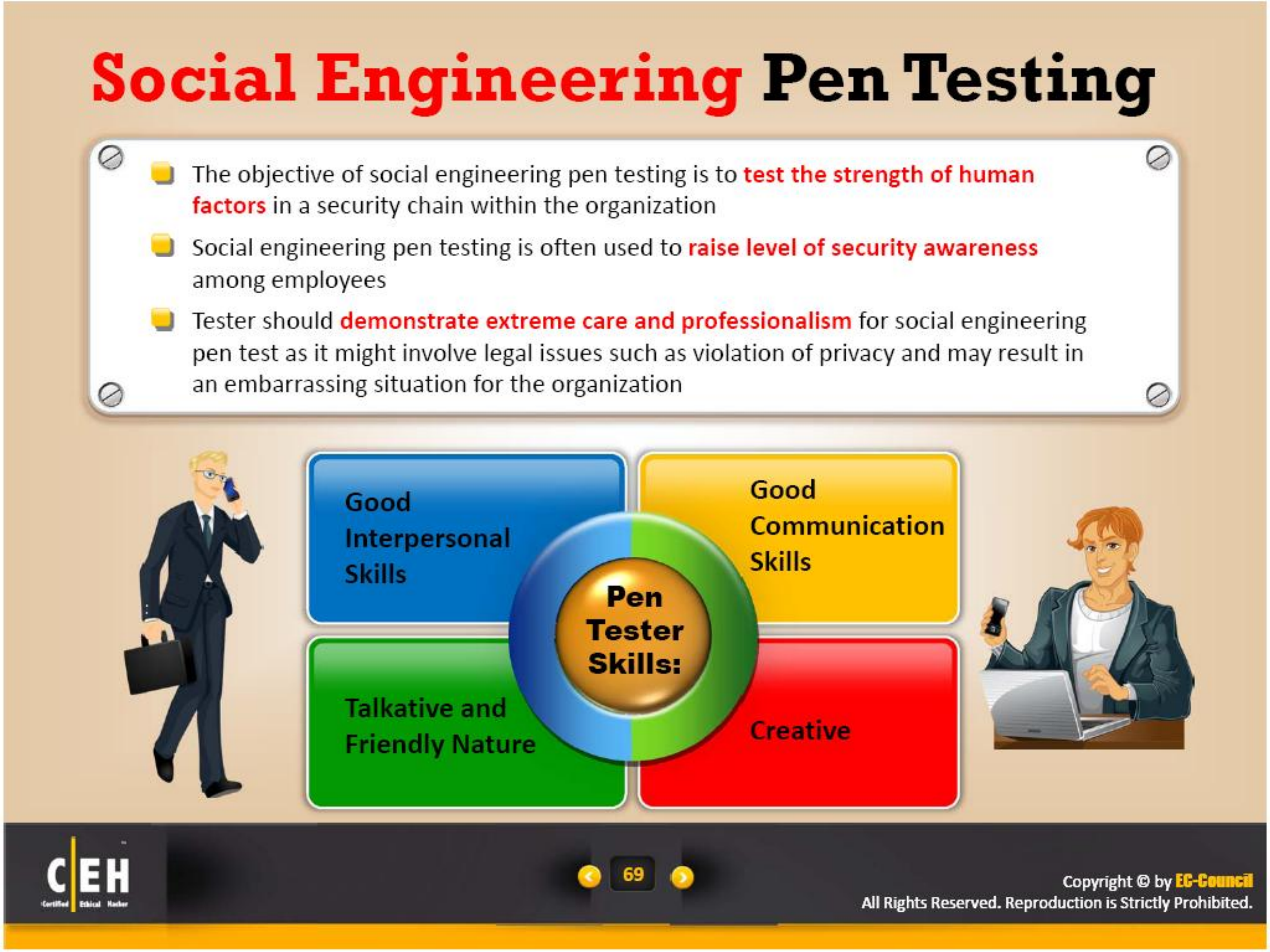
Identity Theft Countermeasures

- Secure or shred all documents containing private information
- To keep your mail secure, empty the mailbox quickly
- Ensure your name is not present in the marketers' hit lists
- Suspect and verify all the requests for personal data
- Review your credit card reports regularly
- Never let your credit card out of your sight
- Protect your personal information from being publicized
- Never give any personal information on the phone
- Do not display account/contact numbers unless mandatory



Module Flow

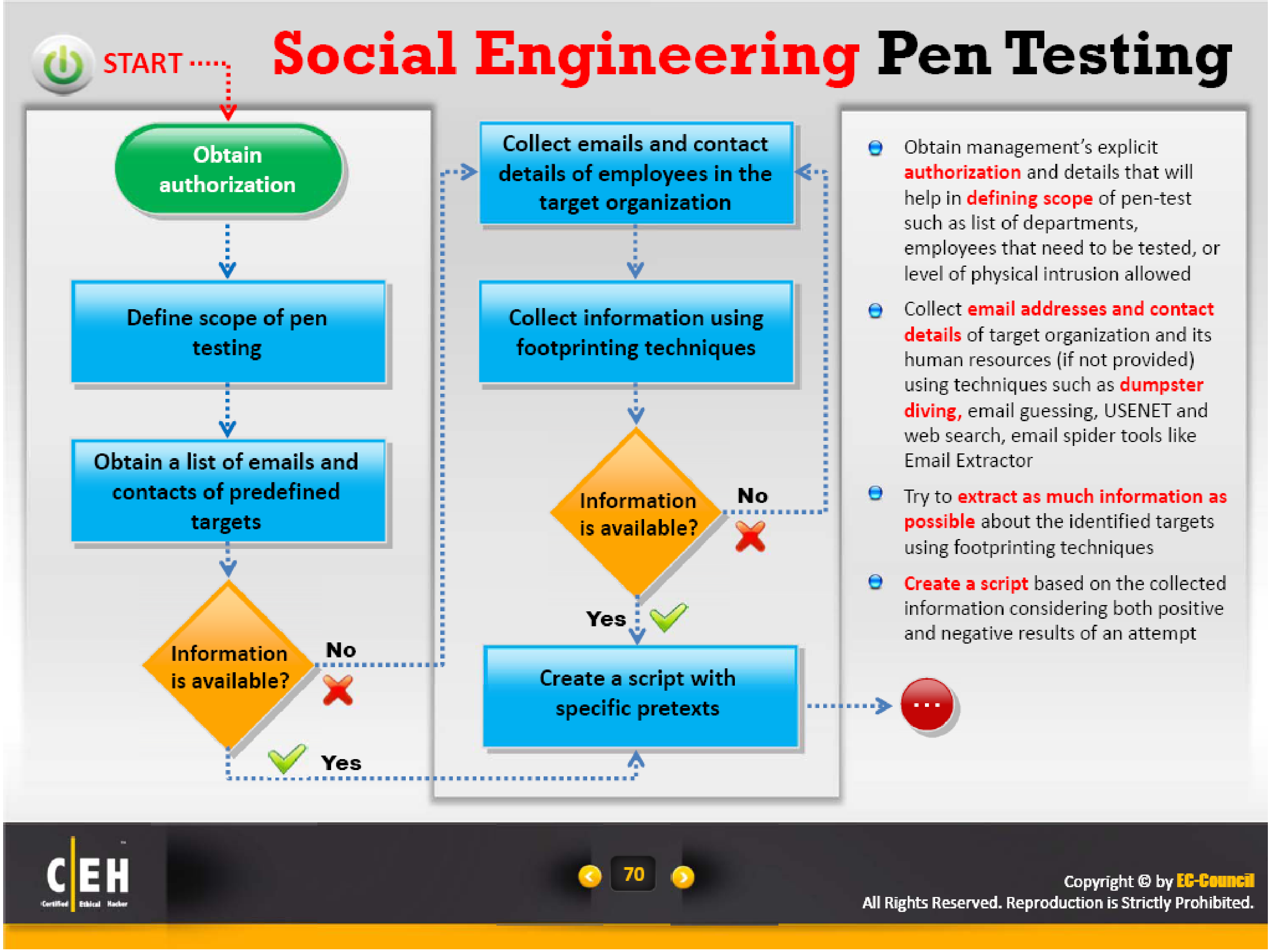
- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing



Social Engineering Pen Testing

- The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization
- Social engineering pen testing is often used to **raise level of security awareness** among employees
- Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization

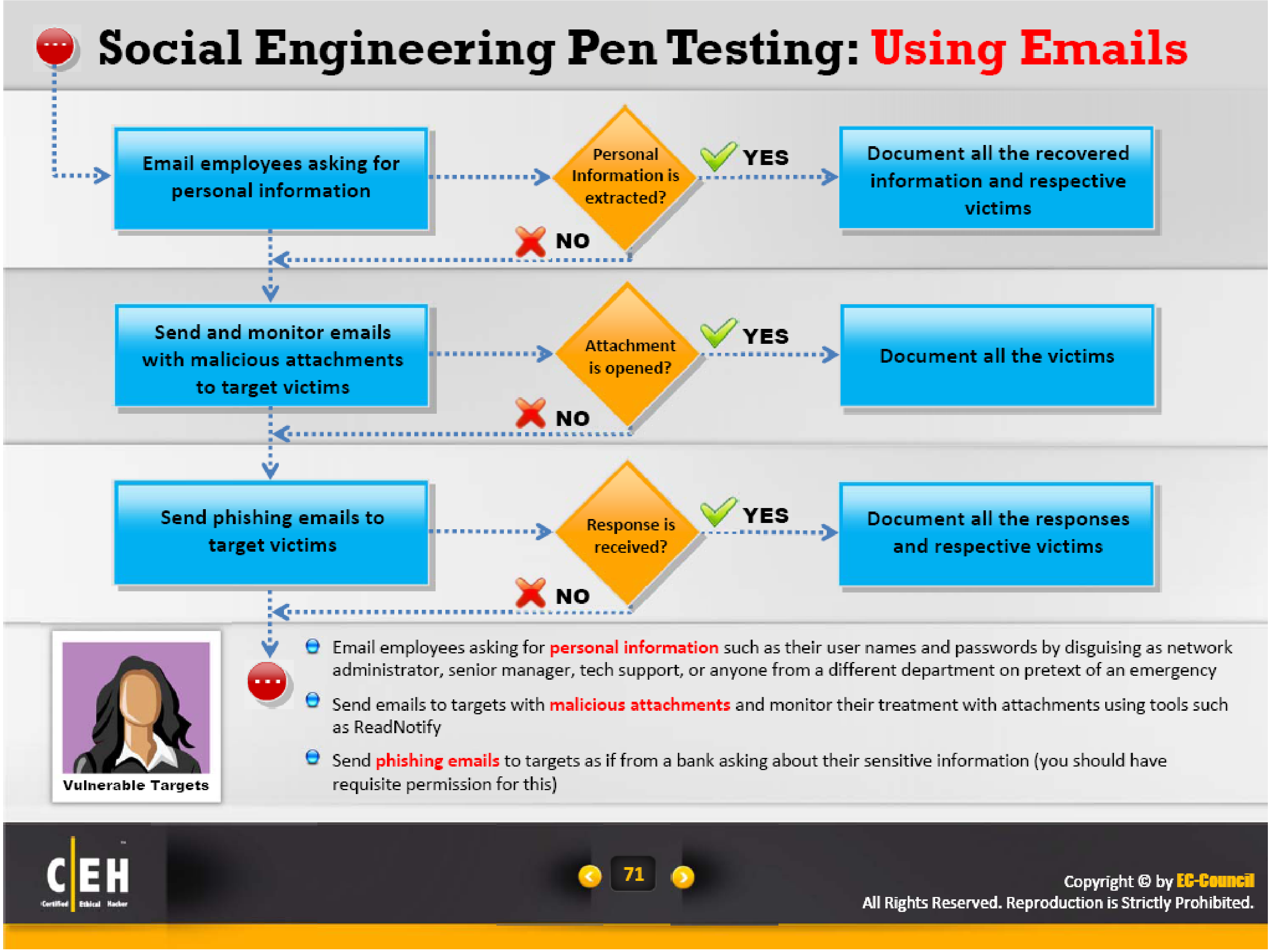
Pen Tester Skills:
Good Interpersonal Skills
Good Communication Skills
Talkative and Friendly Nature
Creative



Social Engineering Pen Testing

START
Obtain authorization
Define scope of pen testing
Obtain a list of emails and contacts of predefined targets
Information is available?
No
Yes
Collect emails and contact details of employees in the target organization
Collect information using footprinting techniques
Information is available?
No
Yes
Create a script with specific pretexts
...

- Obtain management's explicit **authorization** and details that will help in **defining scope** of pen-test such as list of departments, employees that need to be tested, or level of physical intrusion allowed
- Collect **email addresses and contact details** of target organization and its human resources (if not provided) using techniques such as **dumpster diving,** email guessing, USENET and web search, email spider tools like Email Extractor
- Try to **extract as much information as possible** about the identified targets using footprinting techniques
- **Create a script** based on the collected information considering both positive and negative results of an attempt



Social Engineering Pen Testing: Using Emails

Email employees asking for personal information → Personal Information is extracted? → YES → Document all the recovered information and respective victims

NO ↓

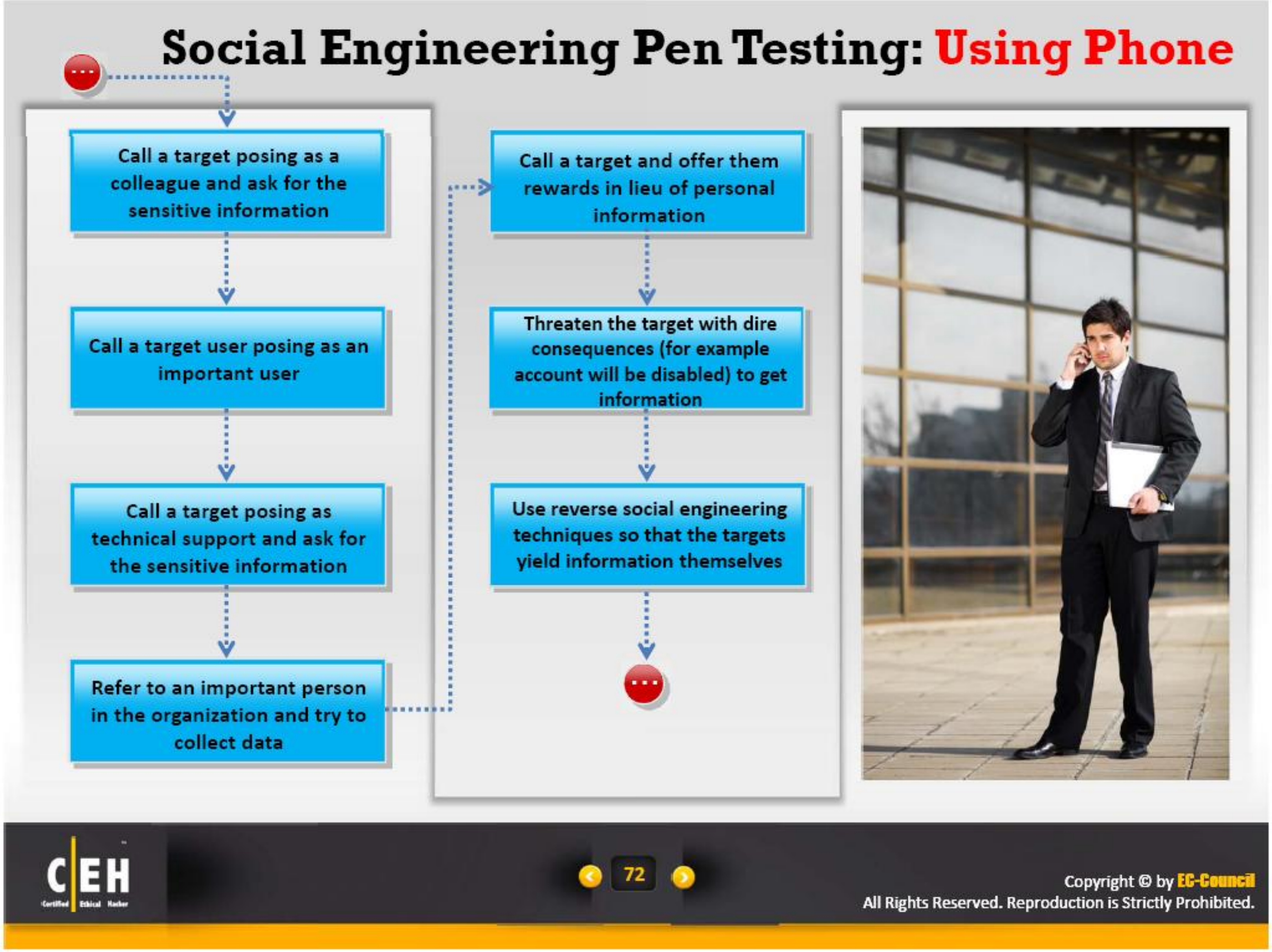
Send and monitor emails with malicious attachments to target victims → Attachment is opened? → YES → Document all the victims

NO ↓

Send phishing emails to target victims → Response is received? → YES → Document all the responses and respective victims

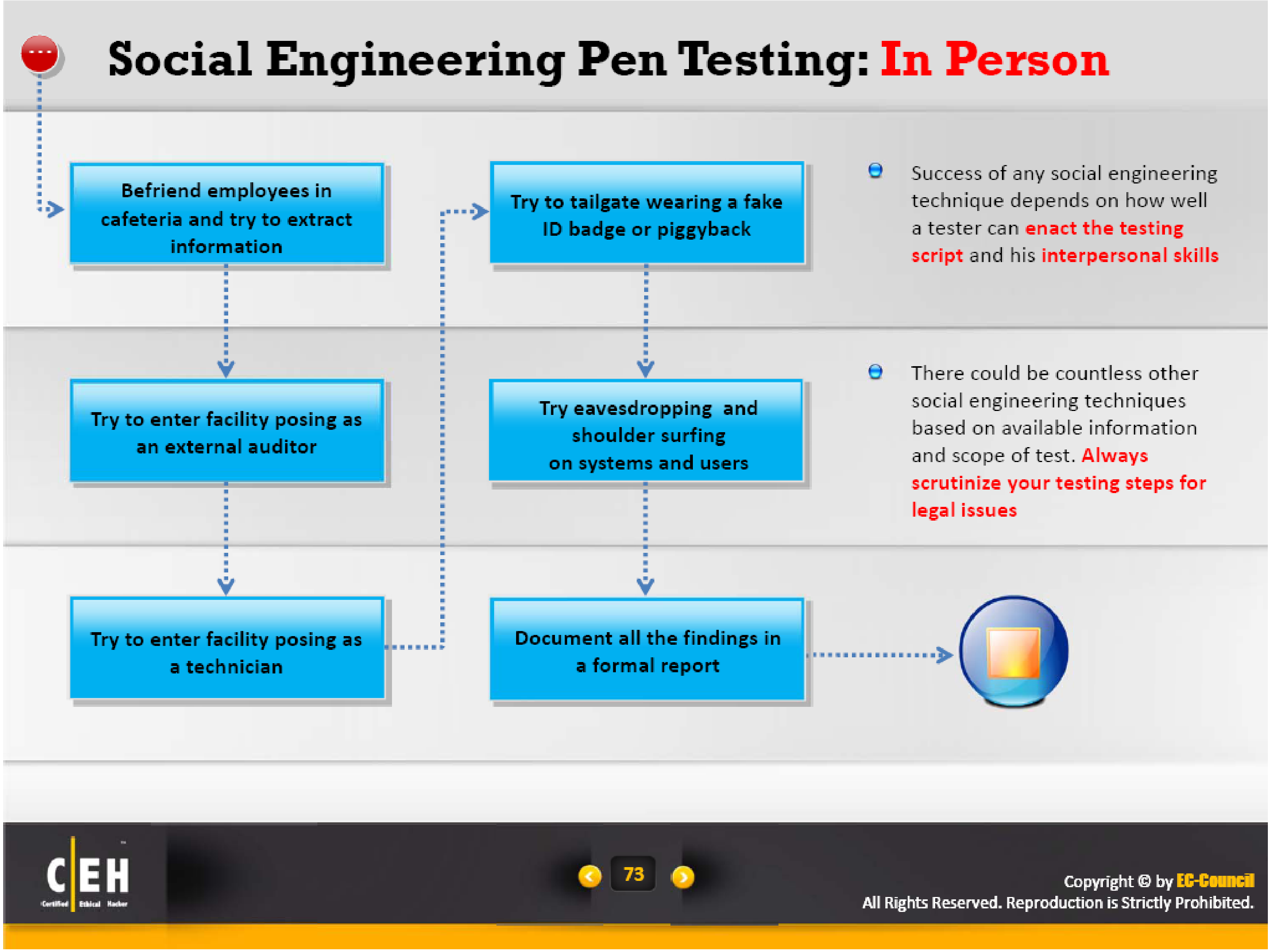
NO ↓

- Email employees asking for **personal information** such as their user names and passwords by disguising as network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency
- Send emails to targets with **malicious attachments** and monitor their treatment with attachments using tools such as ReadNotify
- Send **phishing emails** to targets as if from a bank asking about their sensitive information (you should have requisite permission for this)



Social Engineering Pen Testing: Using Phone

- Call a target posing as a colleague and ask for the sensitive information
- Call a target user posing as an important user
- Call a target posing as technical support and ask for the sensitive information
- Refer to an important person in the organization and try to collect data
- Call a target and offer them rewards in lieu of personal information
- Threaten the target with dire consequences (for example account will be disabled) to get information
- Use reverse social engineering techniques so that the targets yield information themselves



Social Engineering Pen Testing: In Person

Befriend employees in cafeteria and try to extract information

Try to enter facility posing as an external auditor

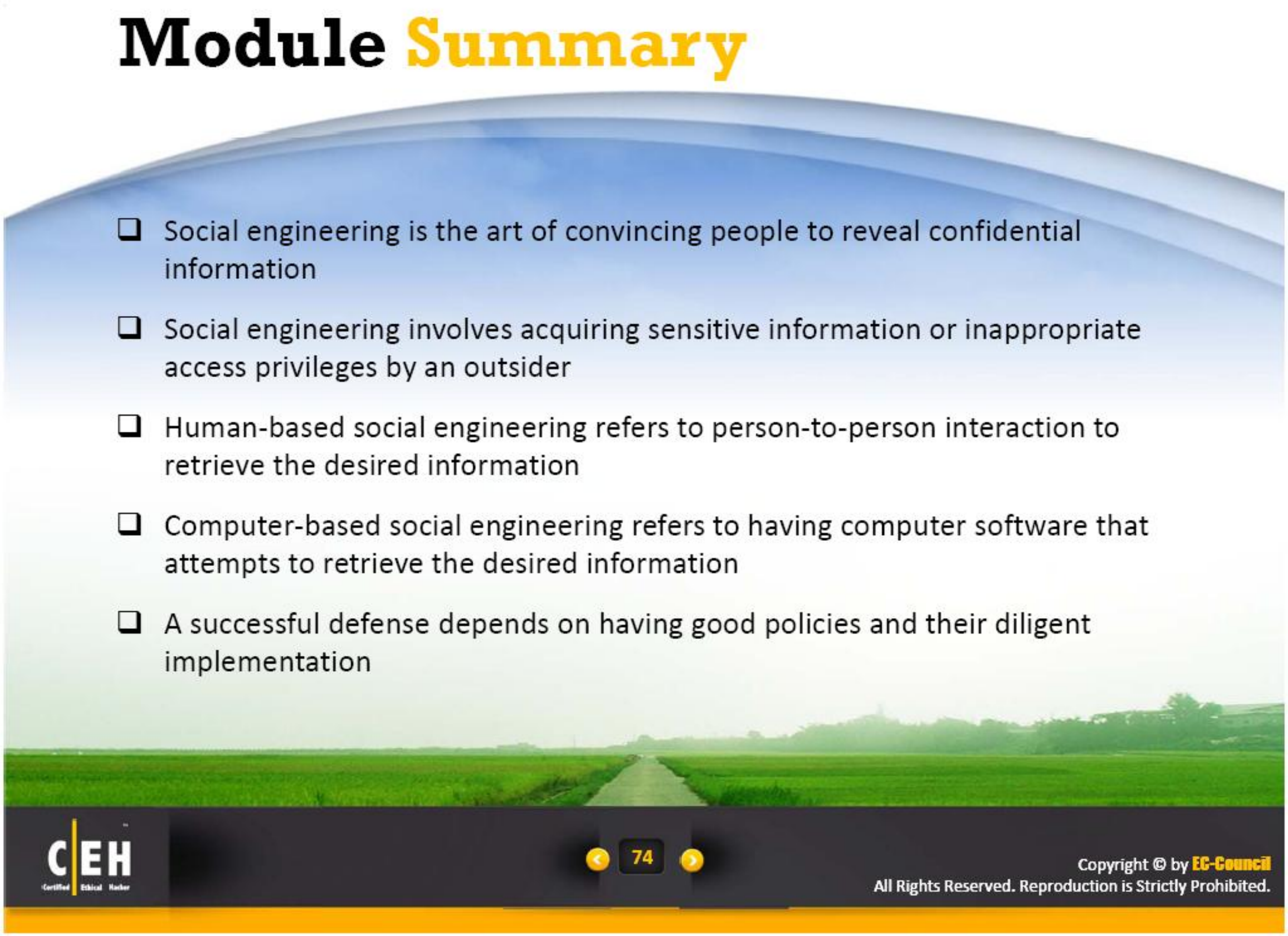
Try to enter facility posing as a technician

Try to tailgate wearing a fake ID badge or piggyback

Try eavesdropping and shoulder surfing on systems and users

Document all the findings in a formal report

- Success of any social engineering technique depends on how well a tester can enact the testing script and his interpersonal skills
- There could be countless other social engineering techniques based on available information and scope of test. Always scrutinize your testing steps for legal issues



Module Summary

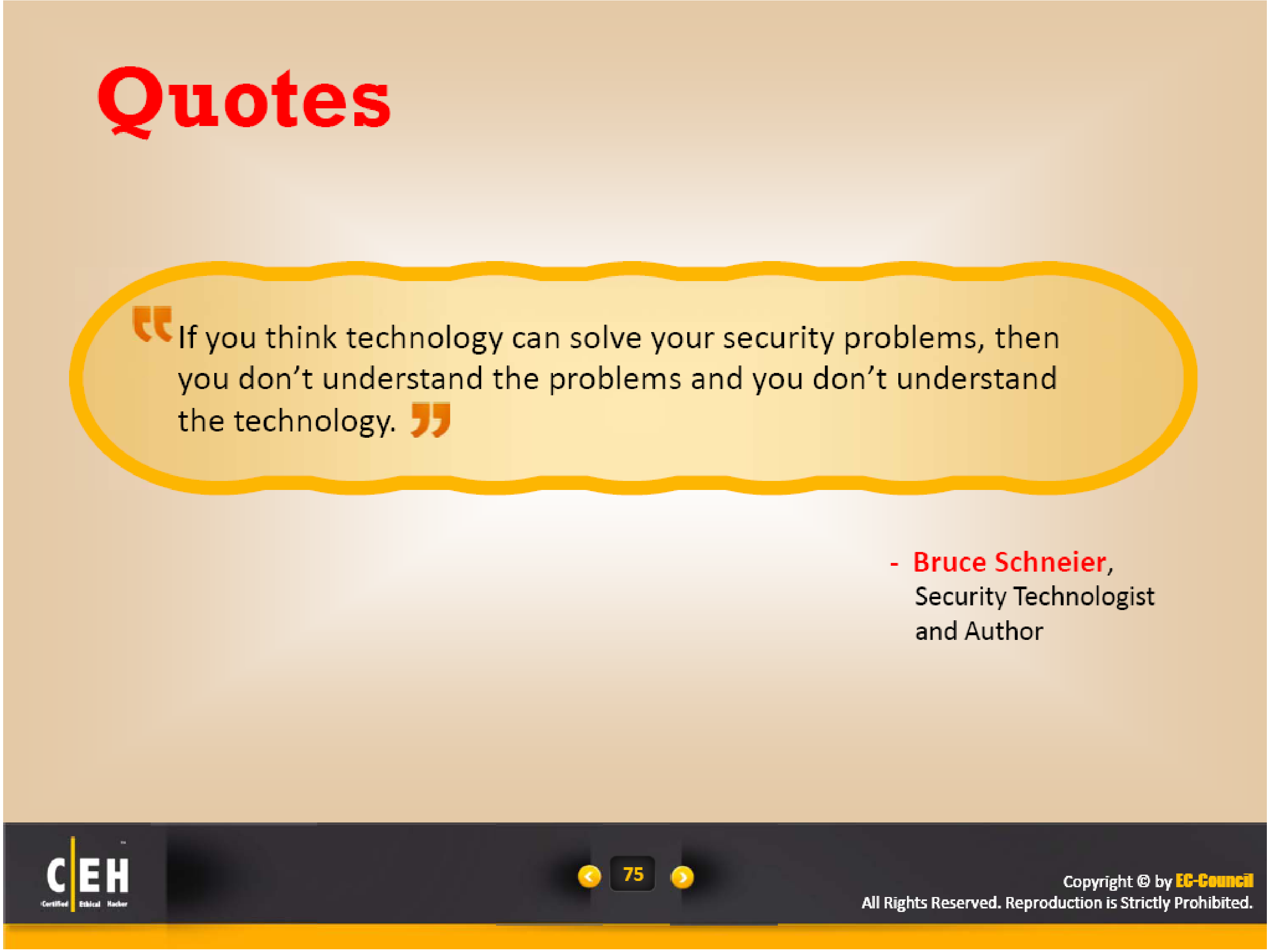
□ Social engineering is the art of convincing people to reveal confidential information

□ Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider

□ Human-based social engineering refers to person-to-person interaction to retrieve the desired information

□ Computer-based social engineering refers to having computer software that attempts to retrieve the desired information

□ A successful defense depends on having good policies and their diligent implementation



Quotes

> If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

- Bruce Schneier,
  Security Technologist
  and Author