

The Role of People in Security: Social Engineering

Slide 1



Principles of Computer Security, Fifth Edition


The Role of People in Security



Social Engineering

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss the role of people in security from the perspective of how the presence of people in the system presents many security problems. In particular, we will discuss social engineering.



Principles of Computer Security, Fifth Edition

People—A Security Problem


- Prevention technologies are not sufficient protection.
- Network and computer systems have human users.
- Humans are error-prone and easily fooled.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The operational model of computer security acknowledges that prevention technologies are not sufficient to protect our computer systems and networks.

The most critical reason for this is that, with only very special exceptions, every network and computer system has at least one human user.

And, as you may know, because you are human: we, humans, are prone to make mistakes and are often easily misled or fooled.



Principles of Computer Security, Fifth Edition


Social Engineering

- Convincing an authorized individual to provide confidential information or access to an unauthorized individual.
- Goal: targeted person takes two possible actions:
 - Divulge information to the attacker
 - E.g. secret/private information
 - Do something on behalf of (to the benefit of) the attacker
 - E.g. reset account credentials, send money

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Social engineering is the process of convincing an authorized individual to provide confidential information or access to an unauthorized individual.

Various deceptive practices are used to convince the targeted person to take two possible actions: Divulge information they should not divulge, and convince the target to do something they should not do.



Principles of Computer Security, Fifth Edition

Social Engineering


- Successful because:
 - Most people have a basic desire to be helpful.
 - Individuals normally seek to avoid confrontation and trouble.
- May also be accomplished using other means.
 - E.g. propaganda

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Social engineering is very successful for two general reasons:

Most people have a basic desire to be helpful. And individuals normally seek to avoid confrontation and trouble.

Social engineering may also be accomplished using other means besides direct contact between the target and the attacker.



Principles of Computer Security, Fifth Edition

Social Engineering

- Example approaches:
 - Ask a question
 - Call IT and ask who the manager is
 - Evoke sympathy
 - Need help to avoid trouble with supervisor
 - Appeal to ego
 - You did a great job helping someone else, can you help me, too?
- Insider attacks are more likely to succeed

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

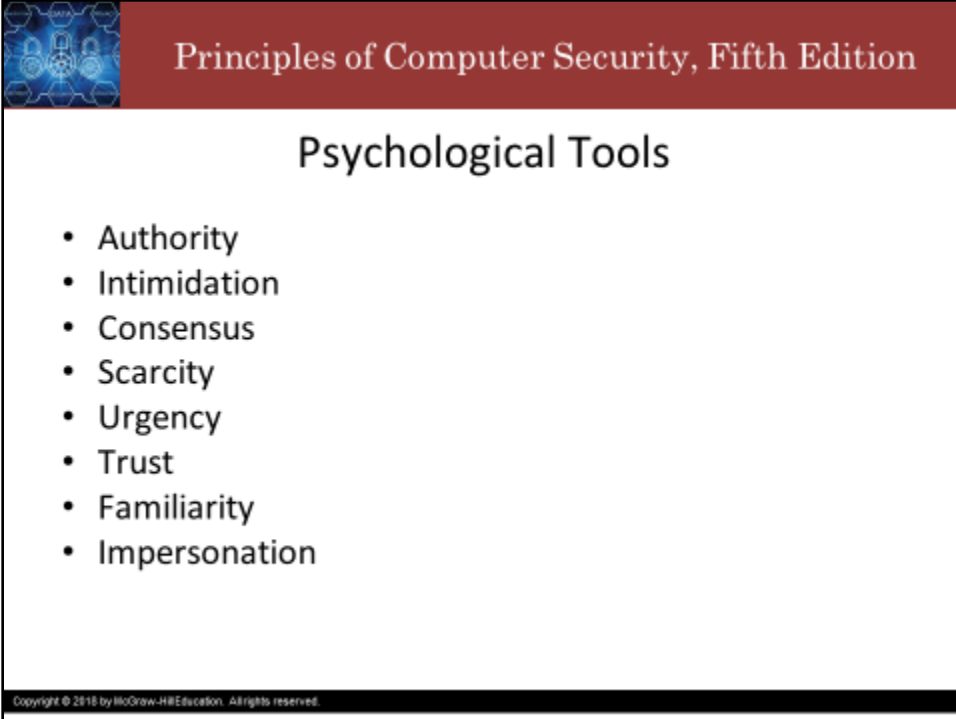
An attacker who is attempting to exploit the natural tendency of people to be helpful may take one of several approaches:

The attacker may simply ask a question, hoping to immediately obtain the desired information.

The attacker may first attempt to engage the target in conversation and try to evoke sympathy so that the target feels sorry for the individual and is more prone to provide the information.

The attacker may appeal to an individual's ego.

Up to this point, social engineering has been discussed in the context of an outsider attempting to gain information about the organization. This does not have to be the case. Insiders may also attempt to gain information they are not authorized to have. In many cases, the insider may be much more successful since they will already have a certain level of information regarding the organization and can therefore better spin a story that may be believable to other employees.



Principles of Computer Security, Fifth Edition

Psychological Tools

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Trust
- Familiarity
- Impersonation

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The tools in a social engineer's toolbox are based on knowledge of human psychology and don't necessarily require a sophisticated knowledge of software or hardware. Over the next few slides, we will see several of the common techniques that social engineers use to hack the human elements of systems.

Some of the more basic and fundamental tools are shown here.

Things like authority – making the victim feel like the attacker has some authority and that challenging that authority will have negative consequences on the victim.

Intimidation is a related tool, where the attacker uses their perceived superiority to pressure the victim. Social engineers often manipulate groups of people to achieve their goal, using consensus helps to mask their involvement.

Creating a perception of scarcity is also a tactic, as is creating a sense of urgency. Advertisers love to use these, too. Only 10 left in stock, order soon! OK Amazon.... Whatever, you say...

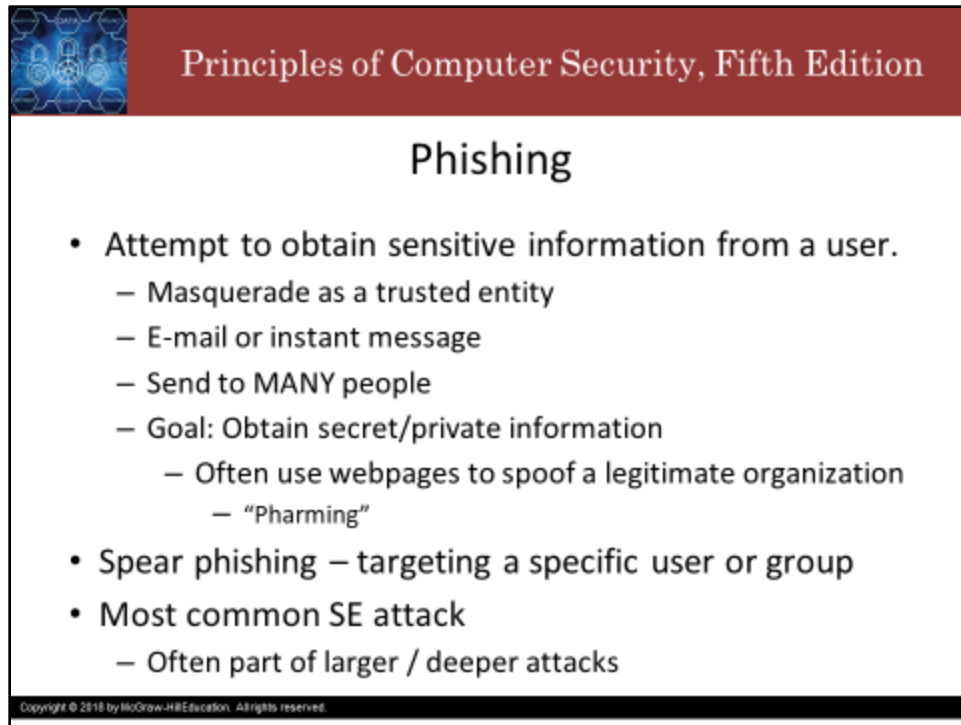
The whole point of social engineering is to build trust – to manipulate people into feeling that they are doing a good or correct thing in the moment.

Building a sense of familiarity is a tool that can lead to misplaced trust – in both the attacker and the victim's own memory and decision making.

Another common tool that involves trust is impersonation, which in other contexts is called spoofing or masquerading. The attacker pretends to be someone or something they are not, and uses the victim's misplaced trust based on that identity or role against them. Common examples of impersonations that social engineers use include Third-party authorization, Help Desk or Tech support, Contractors, and Online attacks like phishing, which we will talk more about very soon.

The best defense against impersonation is to integrate identification verification into the organizational culture. Then, anyone without ID or who takes offense to being asked to provide ID is easily detected as suspicious.

Slide 7



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the word "Phishing" is centered in a large, bold, black font. The main content consists of a bulleted list of characteristics of phishing attacks. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

- **Attempt to obtain sensitive information from a user.**
 - Masquerade as a trusted entity
 - E-mail or instant message
 - Send to MANY people
 - Goal: Obtain secret/private information
 - Often use webpages to spoof a legitimate organization
 - “Pharming”
- **Spear phishing – targeting a specific user or group**
- **Most common SE attack**
 - Often part of larger / deeper attacks

Phishing is a type of social engineering attack in which an attacker attempts to obtain sensitive information from a user by masquerading as a trusted entity in an e-mail or instant message sent to a large group of users.


The attacker attempts to obtain things like usernames, passwords, credit card numbers, and details about the user's bank accounts.

Often, the message from the attacker points the victim to a fake web site which extends the masquerade and collects the information – since you would never give your bank account credentials over email, but you wouldn't blink to put them into a form on a website that looks exactly like your banks' homepage. Although, many phishing victims fall for astonishingly basic and obvious ploys. This tactic, of redirecting users to attack sites, is known as pharming.

A specialized version of phishing is spear phishing. In a spear phishing attack, specific individuals are targeted, usually people in important or critical roles in an organization such as the corporate officers or system administrators, or even the custodial crew who have physical access to the facility. The goal is to go after these specific and high-value targets in a way that is somewhat tailor-made for the intended victims.

When the target has a high-profile, like a C-level executive, the attack is sometimes called whaling. Phishing is now the most common form of social engineering attack related to computer security. The target may be a computer system and access to the information found on it (such as is the case when the phishing attempt asks for a user ID and password) or the target may be personal information, generally financial, about an individual (in the case of phishing attempts that ask for an individual's banking information). An important point to keep in mind is social engineering may only be part of the attack and it may be used throughout the lifecycle of the attack. Some of the most exciting hacker stories involve social engineering (tech is boring, people are dramatic). Kevin Mitnick has some good stories from his heyday.

Slide 8



Principles of Computer Security, Fifth Edition

Vishing

- Phishing that uses voice communication.
- Takes advantage of trust in the telephone network.
 - Attackers can spoof calls from legitimate entities using Voice over IP (VoIP) technology.
- Identity theft is a common objective

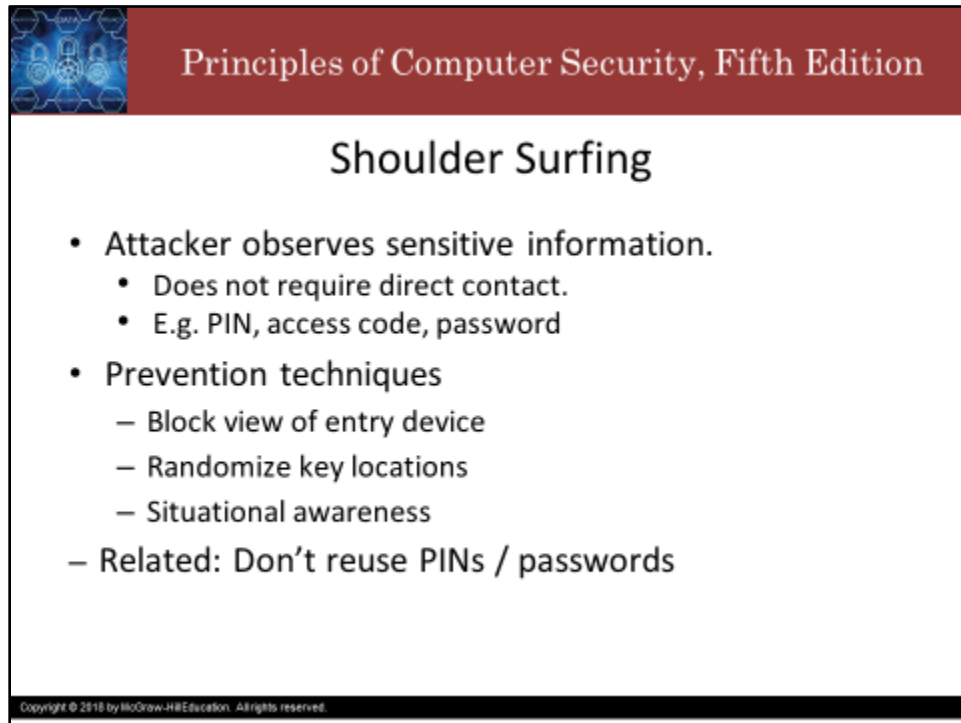
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking. Vishing, the term, is a combination of “voice” and “phishing”. Vishing is generally successful because of the trust that individuals place in the telephone system. With caller ID, people believe they can identify who it is that is calling them. They do not understand that, just like many protocols in the TCP/IP protocol suite, caller ID can be spoofed.

The user may receive a call from, or an e-mail asking them to call a number that is answered by, a potentially compromised voice message system. Users may also receive a recorded message that appears to come from a legitimate entity. In both cases, the user will be encouraged to respond quickly

and provide the sensitive information so that access to their account is not blocked. If a user ever receives a message that claims to be from a reputable entity and asks for sensitive information, the user should not provide it but instead should use the Internet or examine a legitimate account statement to find a phone number that can be used to contact the entity. The user can then verify that the message received was legitimate or report the vishing attempt.

Slide 9



Principles of Computer Security, Fifth Edition

Shoulder Surfing

- **Attacker observes sensitive information.**
 - Does not require direct contact.
 - E.g. PIN, access code, password
- **Prevention techniques**
 - Block view of entry device
 - Randomize key locations
 - Situational awareness
- **Related: Don't reuse PINs / passwords**

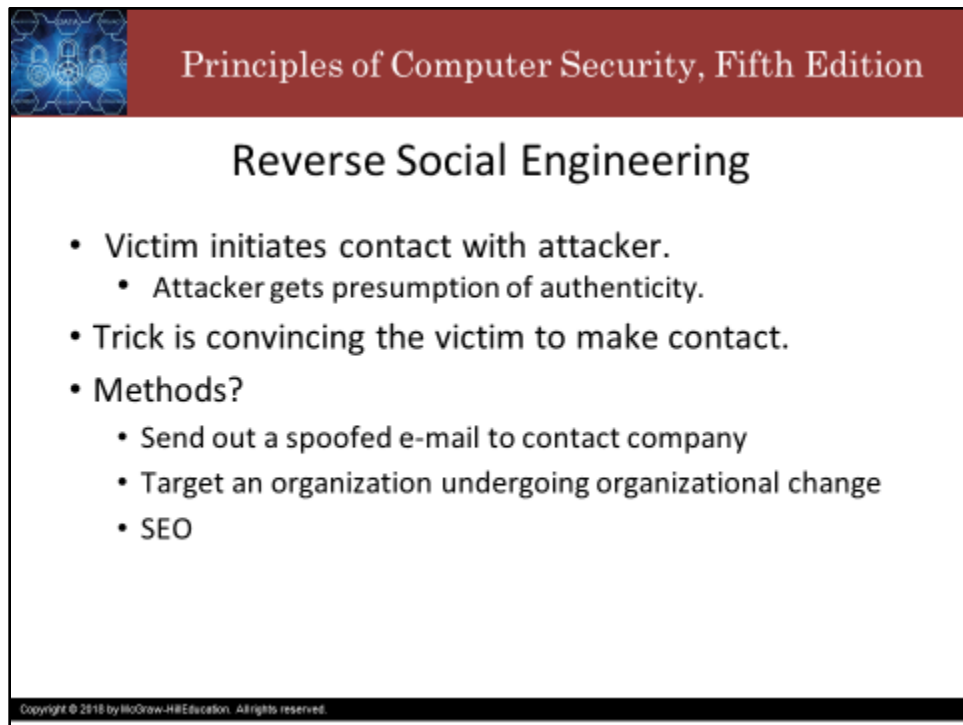
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In a shoulder-surfing attack, the attacker observes the victim entering sensitive information on a form, keypad, or keyboard or sets up a camera or uses binoculars to view the user entering sensitive data. It does not require direct contact between the attacker and victim.

Common examples of information that gets shoulder surfed includes PINs and access codes and even passwords.

Shoulder surfing prevention techniques include things like putting a shield over the keypad, scrambling the location of the symbols on the keypad, and maintaining awareness of the people or devices which can see the data.

A related, and hopefully obvious, security precaution is that a person should not use the same PIN for all of their accounts since an attacker who learns the PIN for one type of access could then use it for another type of access.



Principles of Computer Security, Fifth Edition

Reverse Social Engineering


- Victim initiates contact with attacker.
 - Attacker gets presumption of authenticity.
- Trick is convincing the victim to make contact.
- Methods?
 - Send out a spoofed e-mail to contact company
 - Target an organization undergoing organizational change
 - SEO

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Reverse social engineering occurs when the attacker hopes to convince the victim to initiate the contact.

One reason this attack might be successful is that, since the victim is initiating the contact, the attacker may not have to do anything more to convince the victim of their authenticity.

The tricky part of this attack is convincing the victim to make that initial contact. Possible methods to accomplish this might include sending out a spoofed e-mail (fake e-mail designed to appear authentic) that claims to be from a reputable source and provides another e-mail address or phone number to call for “tech support,” or posting a notice or creating a bogus web site for a legitimate company that also claims to provide “tech support.” This may be especially successful if timed to coincide with a company’s deployment of a new software or hardware platform. Another potential time to target an organization with this sort of attack is when there is a significant change in the organization itself, such as when two companies merge or a smaller company is acquired by a larger one. During these times, employees are not familiar with the new organization or its procedures, and amidst the confusion, it is easy to conduct either a social engineering or reverse social engineering attack. Another nasty trick is to use search engine optimization techniques to make the attack site (or contact information) appear high up in the search results for keywords the victim is likely to use. Picking these keywords involves a lot of psychology, but in a whaling operation, a good list will include the target’s own name.



Principles of Computer Security, Fifth Edition

Hoaxes

- Can be very damaging if victim takes action that weakens security
- Best defense: training and awareness
 - Be suspicious of unusual e-mails and stories
 - Know who to contact in the organization for verification
 - Don't spread the hoax


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Hoaxes may be considered merely a nuisance and not really a security problem. But, they can actually cause a lot of damage. This is also true for disinformation campaigns that attempt to discredit legitimate information by calling it a hoax.

The best and first line of defense for both users and administrators against hoaxes is training and awareness.

Users should be trained to be suspicious of unusual e-mails and stories and should know who to contact in the organization to verify their validity when received.

Hoaxes often advise the user to send it to their friends so they know about the issue as well—and by doing so, they help spread the hoax.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Hit **Alt+F4** or **Cmd+W** to show your support.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

You are amazing. It would really mean a lot to me if you would show your support by pressing the alt and f4 keys at the same time (or command and w on a Mac). Spread the word! Thank you and take care.

The Role of People in Security: Poor Security Practices

Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the main title "The Role of People in Security" is displayed in a large, black, sans-serif font. Underneath the title is a photograph of a woman with dark hair, wearing a black office chair, looking over the top of the chair with a concerned expression. Below the photograph, the subtitle "Poor Security Practices" is written in a black, sans-serif font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we continue our discussion of the role of people in security by talking about security practices.



Principles of Computer Security, Fifth Edition


Poor Security Practices

(good penetration testing vectors)

- Bad Password Selection
- Shoulder Surfing
- Piggybacking
- Dumpster Diving
- Installing Unauthorized Hardware or Software
- Improper Data Handling
- Physical Access by Non-Employees
- Violation of Clean Desk Policies

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A significant portion of human-created security problems result from poor security practices. These poor practices may be due to an individual user who is not following established security policies or processes or they may be caused by a lack of security policies, procedures, or training within the user's organization.



Principles of Computer Security, Fifth Edition

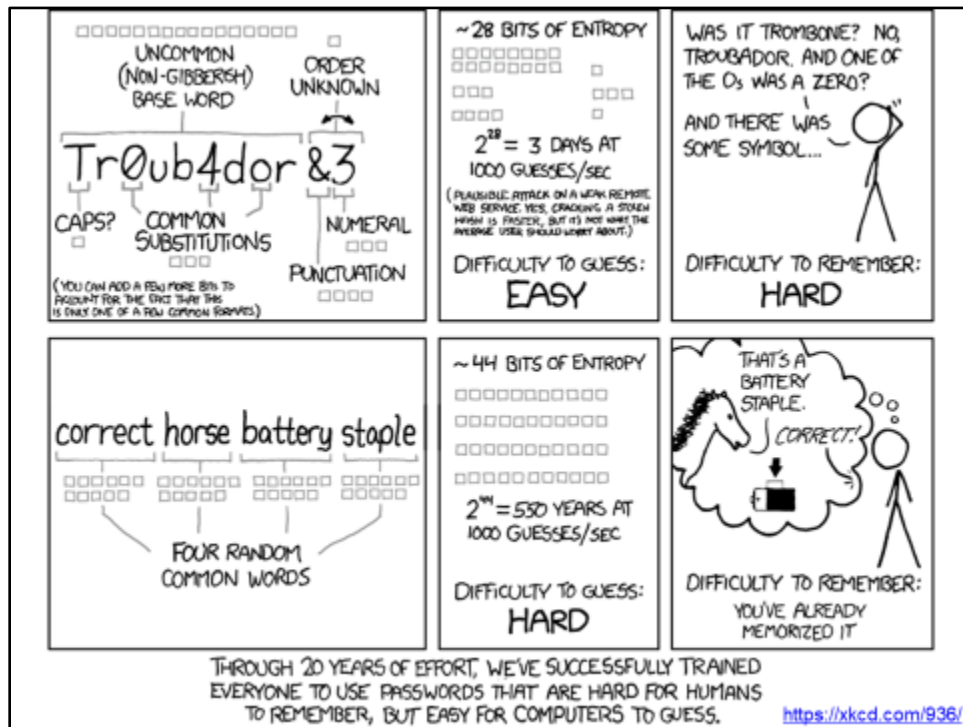
Password selection

- Average user has weak passwords
 - Average user with a strong password does not keep it secure.
- Organization's password policy often at odds with usability
- Strong passwords are long, use the full character set, and are never reused
 - Good: long and memorable, but not common
 - Better: long, complex, unknown, and kept by secure password manager (to which the password is long, memorable and not common)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Poor password selection is one of the most common of poor security practices, and one of the most dangerous. Numerous studies that have been conducted on password selection have found that, while overall more users are learning to select good passwords, a significant percentage of users still make poor choices. The problem with this, of course, is that a poor password choice can enable an attacker to compromise a computer system or network more easily. Even when users have good passwords, they often resort to another poor security practice—writing the password down in an easily located place, which can also lead to system compromise if an attacker gains physical access to the area. Organizations have instituted additional policies and rules relating to password selection to further complicate an attacker's efforts. Organizations may require users to change their password frequently. This is so that if an attacker is able to compromise a password, it is only valid for a limited period of time before a new password is selected, after which the attacker is locked out. All is not lost for the attacker, however, since, again, the average user will select another weak password they can remember.

Another policy or rule governing password selection often adopted by organizations is that passwords must not be written down. This, of course, is difficult to enforce, and thus users will frequently write them down, often as a result of what is referred to as the "password dilemma." The more difficult we make it for attackers to guess our passwords by making them long and complex, and the more frequently we force password changes, the more difficult the passwords are for authorized users to remember and the more likely they are to write them down. Writing them down and putting them in a secure place is one thing, but all too often users will write them on a slip of paper and keep them in their calendar, wallet, or purse.



You should know the rules for good password selection. Generally, these are to use at least eight characters in your password, include a combination of upper and lowercase letters, include at least one number and one special character, do not use a common word, phrase, or name, and choose a password that you can remember so that you do not need to write it down. The best advice, though, is to pick a long and memorable passphrase. The length of the password is the most important factor for security against an attacker. The memorability of the password is the most important factor for psychological acceptability.

Another suggestion, and this is what I actually do myself, is to have a password manager that securely stores your passwords so that you don't have to remember them. This way you only have one (very strong) password to remember, which is the password to unlock the password manager's storage. All the other passwords can be long, complex, unique, and utterly unmemorable. For example, I do not know most of the passwords to the sites on which I have accounts. They are too long and too complex and there are too many of them to remember. If someone wants my bank password, they won't get it from me, because I literally don't know it.



Principles of Computer Security, Fifth Edition

Piggybacking


- Tailgating or piggybacking is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.
 - An attacker can gain access to the facility without having to know the access code or having to acquire an access card.
 - Prevent tailgating by using procedures ensuring nobody follows too closely or is in a position to observe actions.
 - Can use a “person trap,” which utilizes two doors to gain access to the facility

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Piggybacking is related to social engineering attacks. Both the piggybacking and shoulder surfing attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions. Both of these rely on the poor security practices of an authorized user, such as people are often in a hurry and will frequently not follow good physical security practices and procedures.

Attackers know this and may attempt to exploit this to gain access to the facility without having the access code or card.

One effective defensive structure is a *person trap*, which utilizes two doors to gain access to the facility. The second door does not open until the first one is closed and is spaced close enough to the first that an enclosure is formed that only allows one individual through at a time.



Principles of Computer Security, Fifth Edition

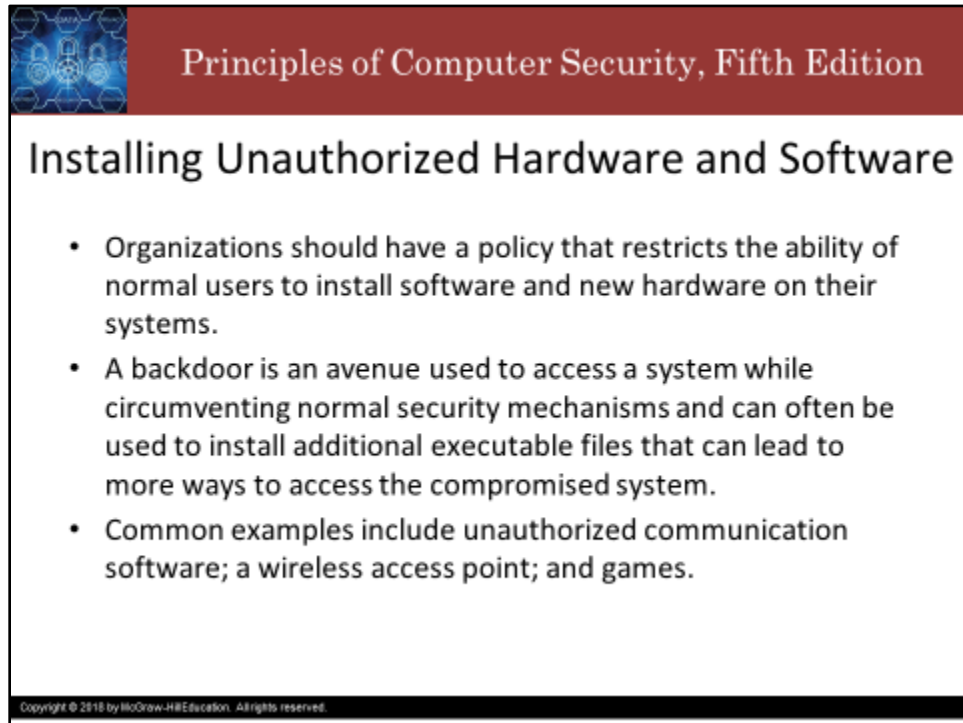
Dumpster Diving

- Dumpster diving is the process of going through a target's trash in hopes of finding valuable information.
 - Has been used by identity thieves, private investigators, and law enforcement personnel, to obtain information about an individual or organization
 - May actually find user IDs and passwords
 - Will probably find employee names, from which it's not hard to determine user IDs
 - May gather a variety of information that can be useful in a social engineering attack

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Attackers need a certain amount of information before launching an attack. One common place to find this information, if the attacker is geographically near the target, is the target's trash.

In most locations, trash is not considered private property after it has been discarded (and even where dumpster diving is illegal, little actual enforcement occurs). An organization should have policies about discarding materials. Sensitive information should be shredded and the organization should consider securing the trash receptacle so that individuals can't forage through it. People should also consider shredding personal or sensitive information that they wish to discard in their own trash. A reasonable quality shredder is inexpensive and well worth the price when compared with the potential loss that could occur as a result of identity theft.

A slide from the textbook "Principles of Computer Security, Fifth Edition". The slide has a dark red header with the title "Principles of Computer Security, Fifth Edition" in white. Below the header is a blue graphic with a grid of icons. The main content area is white with a black border. The title "Installing Unauthorized Hardware and Software" is in bold black text. Below it is a bulleted list of three items. At the bottom left, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Installing Unauthorized Hardware and Software

- Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems.
- A backdoor is an avenue used to access a system while circumventing normal security mechanisms and can often be used to install additional executable files that can lead to more ways to access the compromised system.
- Common examples include unauthorized communication software; a wireless access point; and games.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

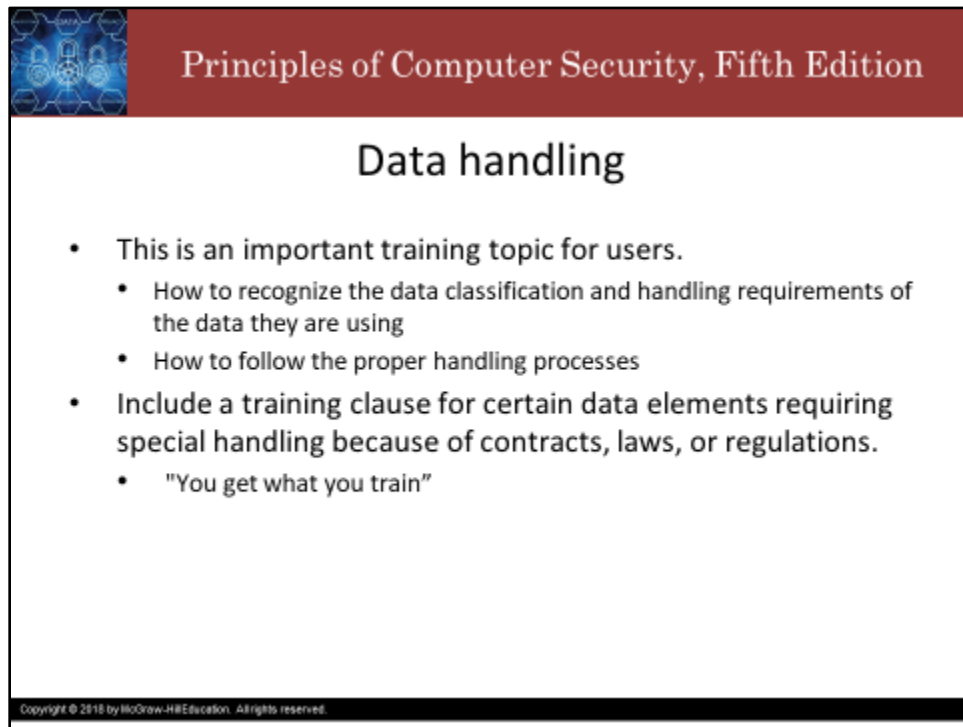
Organizations should have a policy that restricts the ability of normal users to install software and hardware on their systems.

A common example is a user installing unauthorized communication software to allow them to connect to their machine at work from their home. It's 2021 as I record this and the world is still dealing with the SARS-CoV2 pandemic which forced many people to work from home, so such software is now common on many systems.

Another common example is a user installing a wireless access point so that they can access the organization's network from many different areas. In these examples, the user has set up a backdoor into the network, circumventing all the other security mechanisms in place. This is referred to as a "rogue access point".

Another common example of unauthorized software that users install on their systems is games. Games downloaded from the Internet may contain malware.

Because of these potential hazards, many organizations do not allow their users to install software or hardware without the knowledge and assistance of administrators. Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments that are sent to users. This helps prevent users from, say, unwittingly releasing a worm or virus into the system. Consequently, many organizations have their mail servers strip off executable attachments to e-mail so that users can't accidentally cause a security problem.



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of blue gears and a padlock. The main content area is white with the title "Data handling" in black. Below the title is a bulleted list. At the bottom of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Data handling

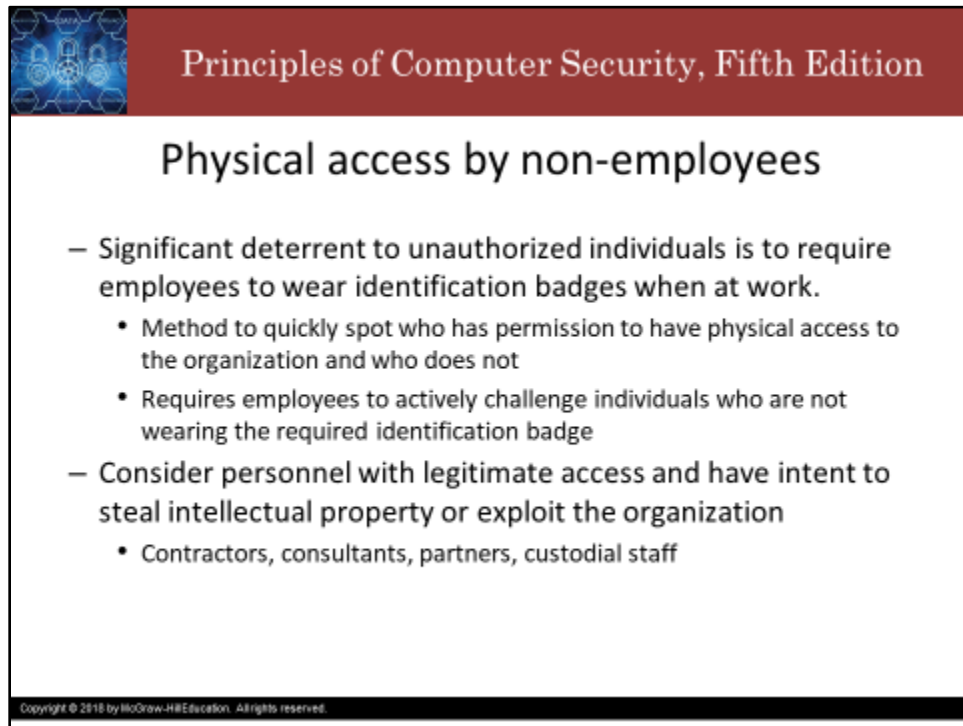
- This is an important training topic for users.
 - How to recognize the data classification and handling requirements of the data they are using
 - How to follow the proper handling processes
- Include a training clause for certain data elements requiring special handling because of contracts, laws, or regulations.
 - "You get what you train"

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Understanding the responsibilities of proper data handling is an important training topic for users.

They typically need training in how to recognize the data classification and handling requirements of the data they are using and how to follow the proper data handling processes.

If certain data elements require special handling due to contracts, laws, or regulations, there is typically a training clause associated with this requirement. Personnel assigned to these tasks should be specifically trained with regard to the security requirements. The spirit of the training clause is "you get what you train"; if security of specific types of data is a requirement, then users should be trained to handle it properly.

The slide features a dark red header with the title "Principles of Computer Security, Fifth Edition" in white serif font. On the left side of the header is a decorative graphic of blue and white geometric patterns. The main content area is white with a black border. The title "Physical access by non-employees" is centered in a large, bold, black sans-serif font. Below the title is a list of bullet points. The first bullet point is a hyphenated list item, and the second is a hyphenated list item with two sub-bullets. At the bottom left of the slide, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

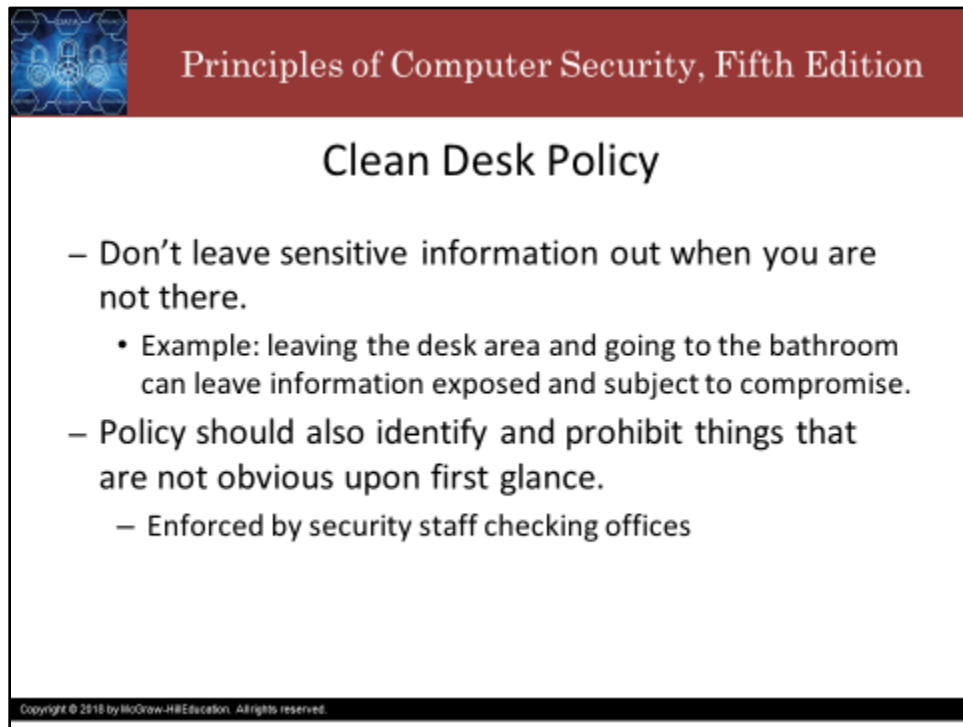
Physical access by non-employees

- Significant deterrent to unauthorized individuals is to require employees to wear identification badges when at work.
 - Method to quickly spot who has permission to have physical access to the organization and who does not
 - Requires employees to actively challenge individuals who are not wearing the required identification badge
- Consider personnel with legitimate access and have intent to steal intellectual property or exploit the organization
 - Contractors, consultants, partners, custodial staff

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

If an attacker gains physical access to a system, their advantage in the attack increases dramatically. Combine an attacker who slips in by piggybacking off of an authorized individual and an environment where employees have not been encouraged to challenge individuals without appropriate credentials and you have a situation where you might as well not have any badges in the first place. Organizations also frequently become complacent when faced with what appears to be a legitimate reason to access the facility, such as when an individual shows up with a warm pizza claiming it was ordered by an employee. It has often been stated by security consultants that it is amazing what you can obtain access to with a pizza box or a vase of flowers.

Another aspect that must be considered is personnel who have legitimate access to a facility but also have intent to steal intellectual property or otherwise exploit the organization. Physical access provides an easy opportunity for individuals to look for the occasional piece of critical information carelessly left out. With the proliferation of devices such as cell phones with built-in cameras, an individual could easily photograph information without it being obvious to employees. Contractors, consultants, and partners frequently not only have physical access to the facility but may also have network access. Other individuals who typically have unrestricted access to the facility when no one is around are nighttime custodial crewmembers and security guards. Such positions are often contracted out. As a result, hackers have been known to take temporary custodial jobs simply to gain access to facilities.

The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. On the left side of the header is a small graphic of blue circuitry. The main content area is white with a black border. The title "Clean Desk Policy" is centered in a large, bold, black font. Below the title is a bulleted list with three main points, each starting with a hyphen. The first point is "Don't leave sensitive information out when you are not there.", followed by an indented sub-point: "• Example: leaving the desk area and going to the bathroom can leave information exposed and subject to compromise." The second main point is "Policy should also identify and prohibit things that are not obvious upon first glance.", followed by an indented sub-point: "– Enforced by security staff checking offices". At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."/>

Principles of Computer Security, Fifth Edition

Clean Desk Policy


- Don't leave sensitive information out when you are not there.
 - Example: leaving the desk area and going to the bathroom can leave information exposed and subject to compromise.
- Policy should also identify and prohibit things that are not obvious upon first glance.
 - Enforced by security staff checking offices

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Preventing access to information is also important in the work area.

Firms with sensitive information should have a “clean desk policy” specifying that sensitive information is not left unsecured in the work area when the worker is not present to act as custodian. Even leaving the desk area and going to the bathroom can leave information exposed and subject to compromise.

The clean desk policy should also identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards and mouse pads or in unsecured desk drawers. In organizations that use a clean desk policy, such as those that work with classified information, the policy is enforced by security staff who check offices and desks when employees leave. The security staff look for anything that was left out that should have been secured. Should they find something, the employee will get a stern talking-to and possibly even lose their job or security clearance.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Keep your passwords strong, check your 6, burn after reading, ID all the people, and keep your desk clean. Thank you and take care.

The Role of People in Security: People as a Security Tool

Slide 1



Principles of Computer Security, Fifth Edition

The Role of People in Security



People As a Security Tool

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The slide features a dark red header with the text 'Principles of Computer Security, Fifth Edition' in white. Below the header, the main title 'The Role of People in Security' is centered in a large, black, sans-serif font. Underneath the title is a photograph of a woman with dark hair, wearing a black office chair, looking over the top edge of the chair's backrest. Below the photograph, the subtitle 'People As a Security Tool' is centered in a black, sans-serif font. At the bottom of the slide, there is a small, black, sans-serif font copyright notice: 'Copyright © 2018 by McGraw-Hill Education. All rights reserved.'

Howdy! In this video, we discuss people as a security tool.




Principles of Computer Security, Fifth Edition

People as a Security Tool

- Social engineering paradox
 - People are not only the biggest problem and security risk but also the best tool in defending against a social engineering attack.
- To fight social engineering attacks, create policies and procedures that establish roles and responsibilities for security administrators and all users.
 - Management expectations, security-wise, from employees
 - Description of items the organization is trying to protect, and mechanisms important for that protection

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An interesting paradox when speaking of social engineering attacks is that people are not only the biggest problem and security risk but also the best tool in defending against a social engineering attack. The first step an organization should take to fight potential social engineering attacks is to create policies and procedures that establish the roles and responsibilities for all users. What is it that management expects, security-wise, from all employees? What is it that the organization is trying to protect, and what mechanisms are important for that protection?




Principles of Computer Security, Fifth Edition

Security Awareness

- Active security awareness program
 - Single most effective method to counter potential social engineering attacks.
 - Extent of training depends on organization's environment and level of threat.
 - Training should stress the type of information that the organization considers sensitive and which may be the target of a social engineering attack.
 - Employees should be aware of attack indicators.
 - Employees should be taught to be cautious about revealing personal information.

Copyright © 2018 by NoStarch-HEEducation. All rights reserved.

A strong security education and awareness training program can go a long way toward reducing the chance that a social engineering attack will be successful. Awareness programs and campaigns, which might include seminars, videos, posters, newsletters, and similar materials, are also fairly easy to implement and not very costly. There is no reason for an organization to not have an awareness program in place. A lot of information and ideas are available on the Internet. See what you can find that might be usable for your organization that you can obtain at no charge from various organizations on the Internet. Make sure to check organizations such as NIST and the NSA, which have developed numerous security documents and guidelines.



Principles of Computer Security, Fifth Edition


Security Awareness

- Corporate security officers
 - Must cultivate an environment of trust as well as an understanding of the importance of security
 - Need the help of all users
 - Should strive to cultivate a team environment in which users, when faced with a questionable situation, will not hesitate to call the security office
- Social Networking and P2P
 - Be careful not to mix social and business communications
 - Don't torrent at work

Copyright © 2010 by McGraw-Hill Education. All rights reserved.

If users feel that security personnel are only there to make their life difficult or to dredge up information that will result in an employee's termination, the atmosphere will quickly turn adversarial and be transformed into an "us versus them" situation. Security personnel need the help of all users and should strive to cultivate a team environment in which users, when faced with a questionable situation, will not hesitate to call the security office. In situations like this, security officers should remember the old adage of "don't shoot the messenger." That is to say, when that reporting a security issue, the reporting party should feel safe to make the report rather than worrying if they'll be held responsible (even if it was something they did to cause the problem). The most important thing is to take action to protect the security goals of the organization without wasting time pinning the blame on a particular individual. Many people are in the habit of sharing too much information online through social media. Everything you post anywhere online, no matter how private you think it is now, is either not private at all or will not be private for long. Social media is a treasure trove for hackers doing reconnaissance. Don't be "that person" who mixes business and personal life and unwittingly divulges information that undermines the organization's security or the security of employees or clients.

Users also need to understand that peer-to-peer file sharing applications, like BitTorrent, can be used as infection vectors and data exfiltration channels.




Principles of Computer Security, Fifth Edition

Security Policy Training and Procedures

- People play a significant role in security.
- Training is important
 - awareness of social engineering
 - desired security habits.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Information security and awareness programs should cover these issues. If the issues are properly explained to users, their motivation to comply won't simply be to avoid disciplinary action for violating a policy, but they will want to positively assist in supporting the security of the organization. People in an organization play a significant role in the security posture of the organization. As such, training is important as it can provide the basis for awareness of issues such as social engineering and desired employee security habits.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care!