A Sample Set of Questions for an Internal Security Survey

Consider the following sample of questions a tool to help you build your own company internal security survey. Complemented by and adapted to your company specifics, they could help you to identify the gaps and challenges that need to be addressed further.

1. What should you do in case of company password disclosure? (multiple choice)
a) Nothing.
b) Immediately change the password.
c) Report it as a security incident.
d) Wait to see if something happens.

Correct answers: b), c)
Substantiation: As written in the Information Security Policy for Employees (please insert reference to your security policies), in case of password disclosure, the employee shall immediately change the password and report the security incident.

2. What is the secure procedure should you lose an access token, key or badge?
a) Enter company premises without verification accompanied by your colleagues or borrow a token/key from a colleague.
b) Wait some time (e.g., a week), and if the token/key still has not been found, report its loss.
c) Immediately report the lost token/key.
d) Request a new visitor access token/key and use that one.

Correct answer: c)
Substantiation: It is necessary to immediately report a lost token/key so it can be disabled to prevent possible misuse and unauthorized entry.

3. How can I protect the confidentiality of sensitive data sent by email?
a) I can add a confidentiality disclaimer at the bottom of the email.
b) By no means; therefore, I do not send sensitive data by email.
c) I can encrypt the email.
d) I can sign the email.

Correct answer: c)
Substantiation: Your email messages can be intercepted by an attacker either as they are stored on an email server or as they travel over the Internet. The digital signature proves to the recipient that you signed the contents of the message and that the contents have not been altered in transit, but it does not make messages unreadable. Encryption renders messages unreadable from the point at which they start their journey to the point at which the intended recipient opens them. You can use encryption features based on digital certificates built into your email service, or you can download another available encryption software (e.g., PGP/GPG).

4. How could your computer become infected with malware? Select all that apply.
a) By running malware that appears to be a legitimate program.
b) By visiting an infected website.
c) Via email – HTML email or attachments (MS Office, PDF).
d) By connecting to an infected network – in a hotel, train, bus or free Wi-Fi hotspot.

Correct answer: a, b, c, d
Substantiation: Running malware that appears to be a legitimate program or mobile application, visiting infected websites, using email and connecting to an infected network are all common ways of having a computer become infected with malware.

5. How can you minimize the amount of spam in your corporate email inbox? Select all that apply.
a) Do not use the company email when registering for various non-work-related services.
b) Post your business email address to public forums.
c) Register only for trusted newsletters.
d) Use your company email exclusively for work-related activities.

Correct answer: a, c, d

Substantiation: If you want to minimize the amount of spam in your corporate email inbox, you should be cautious about posting your corporate email address on public websites, in chat rooms, public forums, social networks and so forth. You should use an email address that is different from your corporate one when using email for your private activities. Reply to email messages only if you trust them. If you do not trust the message and don't trust the sender, verify the legitimacy of the message before responding to it. This also applies to unsubscribing from email distribution lists. Answering spam just confirms to the spammer that your email address is active and legitimate.

6. Which of the following could help you to prevent malware and viruses from infecting your PC?
a) Download software from trusted sources only.
b) Install an antivirus program.
c) Always update your PC when prompted for a system update.
d) All of the above.

Correct answer: d)
Substantiation: All of the choices can be used for preventing malware and viruses from infecting your PC.

7. Where should company devices (monitors, laptops) be located if they are used to process data classified as "Confidential" or "Strictly Confidential"?
a) It is not important.
b) Close to a window.
c) Close to doors.
d) Located in such a way that the processed data cannot be seen by unauthorized personnel.

Correct answer: d)
Substantiation: Devices processing data classified as "Confidential" or "Strictly Confidential"

should be located so as to minimize the risk that the therein-processed data may be seen by unauthorized personnel on display units.

8. What rules/behaviors must be followed when using company mobile phones? Select all that apply.
a) Mobile phone lock policy and password policy.
b) Mobile phone and card encryption.
c) Install any available apps.
d) All of the above.

Correct answer: a, b

Substantiation: Good practice and mobile device management (MDM) policies recommend protecting data on mobile phones against unauthorized physical and logical access by utilizing the following controls:
1. Mobile phone lock policy and password policy.
2. Mobile phone encryption (and also card encryption, if the mobile phone uses a card)
and ensuring that usage of applications outside trusted sources (iTunes, Google Play and MDM market) is forbidden. When installing an application, choose those that have been available and on the market for a longer time, are often downloaded and carry higher ratings of trustability.

9. You are browsing a website over a public Wi-Fi network, but your antivirus program is not updated. Which of the following statements is true?
a) Your device connected to the public Wi-Fi network is still secure because you only access pages containing news from your country.
b) Communication via http cannot be eavesdropped on.
c) Communication to corporate systems via VPN is secure.
d) None of the above statements is true.

Correct answer: d

Substantiation: HTTP is a communication protocol used for communication between a web server and a browser. This protocol does not protect the confidentiality of the transmitted data; data can be eavesdropped on. Infecting your computer is also possible with normal surfing on legitimate websites, and the likelihood of infection is higher if your antivirus, browser or operating system is not updated. The same is true of VPN communication.

10. Which of the following options helps to determine whether an online shopping website is trustworthy?
a) The address of the website starts with “https://.”
b) There's a seal on the website that says “100% secure.”
c) Do a bit of research to see whether the site has a good reputation.
d) Read the website and look for positive reviews from customers.

Correct answer: c)

Substantiation: Malicious sites can also run over https, and security seals can be easily faked. The website owner can also put fake customer reviews on their website. The best option is to do a bit of research to see whether the site has a good reputation. Reputation plays a big role when shopping online. Website credibility should always be a major consideration as part of your considerations when shopping online.

11. What is used in a homoglyphs or homographs attack?
a) Attacker abuses the similarities of character scripts.
b) Attacker sends an infected attachment.
c) Attacker sends the same phishing email to everyone in the company.
d) None of above.

Correct answer: a)
Substantiation: Attackers have started to use new tactics to confuse users. These are called homoglyphs. A homoglyph attack is based on replacing a letter in a URL with another that looks very similar or even identical but belongs to a different alphabet. The human eye does not know the difference, but a computer that perceives each character under a different code name does.

12. Which of the following password-handling activities is secure?
a) Providing the password to your boss on request.
b) Storing the password on paper in an envelope, locked in your desk.
c) Providing the password to internal security on request.
d) Writing the password on a piece of paper and gluing it to the back of your keyboard.

Correct answer: b)
Substantiation: A password that is shared with unauthorized persons is not secure regardless of its length, complexity or other qualities.

13. Which way are users allowed to use their passwords within COMPANY?
a) No restrictions.
b) Passwords should be complex. Users are allowed to use their **COMPANY** passwords outside of **COMPANY**.
c) Passwords should be complex. Users are not allowed to use their **COMPANY** passwords outside of **COMPANY**.
d) Passwords should be complex. Users are allowed to share passwords with their colleagues.

Correct answer: c
Substantiation: Employees must create complex passwords that are long enough and not guessable by an attacker. There are multiple approaches to creating a robust password. One is to remember a sentence, e.g., “I need five coffees to deliver the code today,” and then

change words to numbers or special characters and/or select the first/second/last letter from each word: “I need five coffees to deliver the code today” → “I need 5 coffees 2 deliver the c0d3 today” → “In5c2dtc2day.” The password creation method, as well as the sentence/phrase itself, should be known only to the user of the password. A password used by an employee to access information systems (IS) within COMPANY must not be used to access IS outside COMPANY. Do not share your password with ANYONE: not your colleagues; not your family members, your boss or IT team. Do not tell people your password even when you are on vacation and someone says they urgently need to get access to the system. The IT team is here to handle these situations.

14. You receive a call, and the caller asks for sensitive information. How should you respond?
a) Ask the caller to send this request via a signed email from a company address and verify the caller’s identity.
b) Insist that you call them back on their phone.
c) Ask for the name of their manager before complying with their request.
d) Comply with their request, since they work from home now and don’t have access to a company phone.

Correct answer: a)
Substantiation: Vishing is an attempt to use social engineering over the phone to lure personal or sensitive information out of a user or force them to perform certain actions – e.g., install remote management software and let a “technician” fix the computer. You should ask the caller to send any request for sensitive information via a signed email from a company address, and before replying, you should verify the caller's identity. If the person provides a call-back number or his manager number, it may be part of the scam — so don't use it. Instead, search for the company's official public phone number and call the organization in question.

15. What is the best way to protect the confidentiality of data stored on a laptop in the event the laptop is stolen?
a) Full disk encryption.
b) Anti-theft.
c) Antivirus.
d) Backup.

Correct answer: a)
Substantiation: The best way to protect the confidentiality of data on a laptop is full disk encryption. Anti-theft may help locating the laptop and get it back, but the thief may access data on the hard drive if the disk on the laptop is not encrypted. An antimalware solution does not help in the case of physical theft. Backup is a means to provide availability of data, not its confidentiality.

16. Can I upload, store and process confidential company data in an unauthorized cloud service (Google Docs, Translate, Drive; Dropbox)?
a) Yes.
b) No.

Correct answer: b)

Substantiation: Confidential information can only be stored and processed by a COMPANY IT authorized cloud services provider. Special categories of confidential data cannot be processed even in authorized clouds.

17. What information should not be published on a private social profile? Select all that apply.
a) Information on the internal operations of the organization.
b) Company emails and other contact information.
c) Funny stories about things you have experienced on vacation.
d) Your personal information, such as address and Social Security number.

Correct answer: a, b, d

Substantiation: Information on the internal operations of the organization, company emails and other contact information, and your personal information, such as address and Social Security number, are sensitive information, and it is not appropriate to disclose it.

18. Why do you need to lock your device's screen when it is not in use?
a) To prevent malicious code from automatically installing.
b) To prevent unauthorized people from misusing your access rights to access data on your device.
c) To properly back up data from your device.
d) To comply with copyright law.

Correct answer: b

Substantiation: An unauthorized person has control of the device to the extent of the rights the user has if the device is not locked, i.e., does not require entering a PIN or password for further work. This means that an imposter could gain access to all data stored on that device.

19. Choose which option is NOT a good physical security practice.
a) Employees are obliged to put the equipment into a locked state where it is necessary to log in for further work when the work is interrupted.
b) Employees are obliged to adhere to the principles of clear desk and clear screen.
c) Employees are obliged to carry out service maintenance and repairs on company devices.

d) Employees shall not view sensitive information in areas where unauthorized persons may view it.

Correct answer: c

Substantiation: Good practice guidelines recommend that when you stop working with your device, you should put it in a state where you will need to log in when you return to work; adhere to the clear desk and clear screen principles; and do not view sensitive information in areas where unauthorized persons can see the data displayed. On the contrary, service maintenance and repairs on company devices are performed exclusively by authorized service personnel and should not be undertaken by the employee.

20. How do you perceive the level of your security awareness?
a) Excellent.
b) Good.
c) Weak.
d) Deficient.

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY™