How hard is it to hack?

How hard is it to hack into a computer or network these days?

* 1. About the same as it was 15 years ago
  2. 1 click of a mouse
  3. 2 clicks of a mouse
  4. Incredibly hard

ANSWER: B

What do we mean by targeted email phishing?

* 1. A way of socially engineering you into opening a malicious email, so that you will provide them access to something valuable
  2. You receive an email addressed to you while on a fishing trip
  3. Setting up email marketing campaign for cyber security
  4. None of the above

ANSWER: A

If you click on a link in a malicious phishing email what can the hackers do?

* 1. Access your computer whenever they want
  2. Read all of your emails
  3. Watch everything you do on the Internet
  4. Steal your passwords
  5. All of the above

ANSWER: E

Targeted Email Phishing

What is THE ABSOLUTE most important thing to do when you receive any email that has an embedded hyperlink inside it?

* 1. Obviously, respond to the email
  2. Click the email without checking anything at all
  3. Hover your mouse over the link, and without clicking the link, pay your full attention to see what the ACTUAL URL web address is
  4. Delete the email

ANSWER: C

What are some email fields to ALWAYS review when you receive an email?

* 1. The Date
  2. The From
  3. The To
  4. The Subject
  5. Salutation – how do they address you
  6. Any spelling and grammar mistakes
  7. All of the above

ANSWER: G

You should always believe what you read on your screen, because hackers never ever spoof the “From” field in an email, or the URL website address in your browser:

1. T
2. F

ANSWER: B

Why are phishing pages so successful, in social engineering us for our credentials and personal details?

* 1. They always address us by our first name
  2. They know what time of day we are using our computers
  3. The phishing page can look identical to the legitimate website you think you are visiting
  4. The URL web address itself can look very similar to the legitimate website address you think you are visiting
  5. C & D

ANSWER: E

Always be suspicious if you hover your mouse over a link in an unsolicited email, and notice that is a URL shortener such as Bit.ly or Ow.ly:

1. T
2. F

ANSWER: A

The “From” field in an email can be spoofed by a hacker:

* 1. Very easily
  2. With a ton of effort
  3. After 3 weeks of research
  4. A & C

ANSWER: A

Anytime you are addressed as “Dear Client,” “Dear Customer” or “Hello” you should be:

* 1. Happy
  2. Charmed
  3. Extremely suspicious
  4. Moody

ANSWER: C

What is the main objective for a hacker trying to social engineer you via a phishing email?

* 1. They are hoping you will be distracted and not notice any red flags in the email, such as to where the real URL web address points
  2. That you will start a conversation with them over email
  3. That you have plenty of money to donate to a cause of their choosing
  4. That you will sympathize with their situation

ANSWER: A

If you are required to click a link to visit a website, what is the very first thing you should do when you arrive at that website?

* 1. Always look up at the URL web address in the top browser address bar, to confirm you are at the exact website you were intending to visit
  2. Read the entire URL web address, not just the first few words in it, to see the actual domain where the address is pointing to
  3. Notice how fast you arrived at the website
  4. Marvel at the wonders of the Internet
  5. A & B

ANSWER: E

You should always trust an unsolicited email from a business with a well-known brand, especially if it has a big logo showing.

* 1. T
  2. F

ANSWER: B

Anytime a charity springs up after a natural disaster, and asks for your financial details on their website, you should always treat it with suspicion:

* 1. T
  2. F

ANSWER: A

A large number of websites showing malicious webpages and files are actually benign websites that have been compromised by hackers:

1. T
2. F

ANSWER: A

If you receive an email that you believe is malicious, or trying to phish your credentials, you should:

* 1. Introduce yourself and tell them you know exactly what they are up to
  2. Look for an “unsubscribe” link in the email and click it so they leave you alone
  3. Do not click any unsubscribe link, and never respond to them
  4. Warn your manager, fellow workers, and tell the IT department you received a malicious email
  5. C & D

ANSWER: E

What is the objective of any malicious email that arrives in your inbox, that has a link embedded in it?

1. They want you to click the link
2. Click the link is what they want
3. The link is what they want you to click
4. What they want is the link to be clicked by you
5. All of the above

ANSWER: E

Macros

What are macros in Office Suite files?

* 1. They are files that are very large
  2. Macronutrients are what make up the caloric content of the food you eat
  3. Macros are used to record and automate multi-step tasks so you can execute them all at once
  4. None of the above

ANSWER: C

It would take a number of steps for a malicious macro to execute inside an Office file you receive:

* 1. T
  2. F

ANSWER: B

Why are malicious macros so successful in social engineering us to execute evil code on our computers?

* 1. All it takes is one click of the mouse to enable a malicious macro in an Office file
  2. The hackers were unable to use micros anymore so they reverted back to macros
  3. Because the code is much smaller, it is easier to trick us
  4. None of the above

ANSWER: A

Even though you may use Google Docs, what should you do if you receive an Office file, from the Internet or an untrusted source, that asks you to enable macros?

* 1. Go ahead and enable the macro, because what could possibly go wrong?
  2. Immediately close the document, and inform your manager and IT department that you received such a file
  3. Reply back to the sender and ask them to send another version that is easier to read
  4. None of the above

ANSWER: B

Business Email Compromise (BEC)

What is the goal of Business Email Compromise?

* 1. To persuade you to initiate a wire transfer to a fraudulent bank account
  2. Design a brilliant email marketing campaign
  3. Prevent any emails you send from work being intercepted by your colleagues
  4. Stop any plagiarized email templates from being used

ANSWER: A

Who would they normally want to target at your company?

* 1. People who are very proficient in Microsoft Office and Google Apps products
  2. New hires
  3. People who spend a lot of time on the road doing sales
  4. People who work in Payroll or Accounts Payable

ANSWER: D

How are BEC scammers so successful in social engineering us to send wire transfers?

* 1. The way they communicate to us is very charming
  2. They pretend to be a high-level executive in your company, or a familiar vendor you do business with, and create a sense of urgency to the request
  3. They know so much about your personal life
  4. They promise a return on your investment

ANSWER: B

Which common tricks will a BEC fraudster use to social engineer us?

* 1. They will send adorable gifts a few days before they pull off the scam
  2. They will tell you the request is very urgent, but that they are too busy to discuss it, and it needs to be done ASAP
  3. They will sit in the parking lot for a week and watch who comes and goes from the corporate building
  4. None of the above

ANSWER: B

What should you do if you receive an unexpected urgent message for a big wire transfer from an executive, or a vendor?

* 1. Immediately pick up the phone and verify with the sender that the request is valid
  2. Have a process in place whereby a colleague can help you authorize the transaction together before initiating
  3. Contact your IT and IT Security departments and let them know of the suspicious message
  4. All of the above

ANSWER: D

Instant Messaging

Being hacked, phished or defrauded on a messaging app is way harder to pull off than in email:

* 1. T
  2. F

ANSWER: B

Whenever you see a URL shortener such as bit.ly or ow.ly being displayed in a message, you should:

* 1. Be happy it’s a shortened URL and not a long one
  2. Click it and do whatever they ask you to do
  3. Be very suspicious, especially if it says it is from an official business or government agency
  4. None of the above

ANSWER: C

Always pay attention to your emotions, any time you receive a new unsolicited message:

* 1. T
  2. F

ANSWER: A

Smishing

What exactly is Smishing?

* 1. Breaking a mobile app via text message
  2. Giving someone a huge cuddly hug
  3. Receiving an unsolicited text message
  4. Social engineering via SMS text messages

ANSWER: D

What are some issues when it comes to managing content on your mobile device?

* 1. We tend to see emails and messages on our phones much sooner than we do on our computers
  2. Because of the small screen sizes of mobile devices, it’s harder to see the full URL web address in an email or message
  3. Caller ID numbers can be easily spoofed in SMS text messages
  4. All of the above
  5. B & C

ANSWER: D

Government agencies never send official correspondence in SMS text messages with embedded links, which ask you to reset your login credentials, or share your sensitive details.

* 1. T
  2. F

ANSWER: A

If you know you received a malicious SMS text you should:

* 1. If on a personal phone, delete it
  2. If using a company mobile device, also notify your manager and IT department so they are aware, but do not respond to it
  3. Respond to the text
  4. Click the link in the SMS text
  5. A & B

ANSWER: E

Vishing

What exactly is Vishing?

* 1. Being able to fish using two poles that are positioned in a V-formation
  2. Social engineering for money or personal details using voice phone calls
  3. Using voice calls to hack into people’s mobile phones
  4. A type of vegetarian hummus

ANSWER: B

People who vish usually pretend to be:

* 1. Authority figure
  2. Law enforcement or tax agency
  3. Tech support
  4. A lottery association
  5. All of the above

ANSWER: E

Why is Voice-Over-IP (VOIP) very effective for vishing?

* 1. The scammer can easily spoof the incoming caller ID to make it appear to be a legitimate business
  2. It reduces the monthly bill by 20%
  3. It initiates phone calls between you and the scammer even if reception is poor
  4. Because of VOIP upgrades, you can throw away your old house phone for a more secure one

ANSWER: A

What are some of the tell-tale signs you are being vished:

* 1. They will try to persuade you to grant access to your computer
  2. You will receive a recorded voice mail message threatening you if you do not respond ASAP
  3. They may already know some of your personal details, and will ask you to confirm the missing details
  4. They will pretend to be from the government, or a well-known business
  5. All of the above

ANSWER: E

If you have committed tax fraud, how will the government normally notify you?

* 1. SMS text message
  2. Carrier pigeon
  3. Someone will visit your home
  4. Official government letter
  5. Lawsuit

ANSWER: D

What can you do if you suspect someone is trying to vish you?

* 1. Immediately hang up the phone
  2. Separately call back the business or government agency and ask if you are in trouble
  3. Let your IT and IT Security department know so they can check if others employees have received similar calls
  4. All of the above

ANSWER: D

Ransomware

What exactly are ransomware attacks?

* 1. Fraudsters take you hostage until you give up your files with Bitcoin
  2. It is software that rewards you with a ransom when you use it
  3. Fraudsters take all your files hostage until you pay them
  4. None of the above

ANSWER: C

How does ransomware work?

* 1. The software generates money on the back end while you surf the web
  2. It’s a subscription-based service that stores all your files securely
  3. It holds all your private software keys in a digital vault
  4. The malware scans your computer and then scrambles all your important files so they are unreadable

ANSWER: D

What makes ransomware something that should be taken seriously:

* 1. The encryption is so strong, it is close to impossible to break
  2. The only people who likely have the decryption keys are the bad guys
  3. The chances of finding a decryption tool on the Internet to save you are slim
  4. If you pay the bad guys, they may blackmail you for more money
  5. All of the above

ANSWER: E

What are some ways to respond to a ransomware infection?

* 1. You can wipe your system and restore your important files using a backup copy, stored either in the cloud or on an external drive
  2. You can scour the Internet on the off chance you might find a decryption tool available
  3. You can make sure all your systems are patched and updated to try to prevent future infections
  4. All of the above

ANSWER: D

Cryptomining

What do we mean when we say cryptomining?

* 1. Digging into mountains looking for gold
  2. Using a powerful computer to help maintain a cryptocurrency’s public “blockchain” database, and in return be rewarded with cryptocurrency
  3. Storing the blockchain on your phone
  4. Mining for encrypted software

ANSWER: B

What exactly is crypojacking?

* 1. Digging into mountains looking for gold to steal
  2. Stealing the blockchain on your phone
  3. Mining for encrypted software
  4. Secretly using your computer or mobile phone to help maintain a cryptocurrency’s public “blockchain” database, and in return be rewarded with cryptocurrency

ANSWER: D

Where can cryptojacking code be executed?

* 1. In a mobile app you install
  2. Inside a file that is downloaded
  3. Inside a webpage that you visit
  4. Inside a browser extension you install
  5. All of the above

ANSWER: E

What are the best ways to prevent cryptojacking?

* 1. Be very careful which apps you install on your mobile device?
  2. Install a script blocker into your browser
  3. Do not download any file onto your computer that you don’t completely trust
  4. All of the above
  5. None of the above

ANSWER: D

Red Flags

Anyone can be social engineered because?

* 1. We are all human, and all have triggers that can be exploited
  2. We are all social beings, so we can be engineered
  3. Only a certain demographic can be socially engineered
  4. None of the above

ANSWER: A

Some common emotions the hackers will attempt to trigger are fear, curiosity, immediacy, empathy, and greed:

* 1. T
  2. F

ANSWER: A

What do malicious emails, phone calls and text message all have in common?

* 1. All three of them can all be easily spoofed to appear to come from someone else
  2. They are all sent or received by someone
  3. They are sometimes very dangerous to your health
  4. A and C
  5. None of the above

ANSWER: A

When you receive any email, text or phone call, you should:

* 1. Pause, and take note of your emotions
  2. Look out for any red flags
  3. Immediately reply so you remain professional no matter what
  4. Never fully trust what is presented to you on your phone screen or in email
  5. A, B and D

ANSWER: E

What should your course of action be when you receive unsolicited emails, phone calls or texts that are prompting you to respond?

* 1. Separately open a browser window and visit the establishment’s website, and check your account to see if there is anything that needs to be addressed
  2. Pick up the phone and call the establishment and ask if they sent you the correspondence
  3. Walk into a brick-and-mortar for the establishment and ask them if they sent you the correspondence
  4. All of the above

ANSWER: D

Search Engine Optimization

Google search results for trending topics such as current events, celebrity gossip and natural disasters may contain malicious links implanted on benign websites:

* 1. T
  2. F

ANSWER: A

Any time you type “Free [fill in the blank]” into Google, you should:

* 1. Hope you are showered with free gifts
  2. Be very wary of links to free wallpaper, games, music and screensavers
  3. Know that nothing is really for free on the Internet
  4. B & C

ANSWER: D

There have been many recent instances of Google displaying malicious ads on the top and to the right of the search results?

* 1. T
  2. F

ANSWER: A

When you do a search in Google, you should:

* 1. Check the URL web address for the search result you want to click on, and make sure it is easy to understand and its context relates to what you are searching for
  2. If you already know what site to visit, use bookmarks whenever possible
  3. Avoid clicking on Google ads
  4. Do not trust all search results without vetting them first
  5. All of the above

ANSWER: E

Banking Trojan

How is a banking trojan initially installed?

* 1. You install a malicious mobile app
  2. You download a malicious attachment
  3. You click on a malicious link in an email
  4. All of the above
  5. A & C

ANSWER: D

What does a banking trojan do once installed?

* 1. It monitors your online banking activity
  2. It steals your login credentials
  3. It accesses your bank and add funds to your account
  4. It logs in as you and transfers all your funds out of your account
  5. A, B & D

ANSWER: E

Anytime you see any extra fields in your bank’s login page, asking you for sensitive information, you should NOT log in under any circumstances:

* 1. T
  2. F

ANSWER: A

Fake AntiVirus

Which of these are true about Fake Antivirus:

* 1. The malware presents you with a scary and realistic-looking antivirus screen
  2. The malware pretends you have multiple virus infections
  3. The malware warns that you have no antivirus protection at all
  4. The fake antivirus program will offer to clean up all the infections, but only if you hand over your credit card details
  5. All of the above

ANSWER: E

How can you accidentally install a fake antivirus program?

* 1. You click on a malicious link in an email
  2. You download a malicious attachment
  3. You install a malicious mobile app
  4. All of the above
  5. A & C

ANSWER: D

Apple Computers

Apple Macs are generally more secure than Windows because:

* 1. Apple has a much tighter control on their ecosystem and App Store
  2. Apple owns and controls all of their own hardware and operating system
  3. Windows has a lot more market share, so malware authors generally prefer to write their evil code for the Windows platform
  4. A & C
  5. All of the above

ANSWER: E

Most security issues we experience on Apple computers are due to social engineering:

* 1. T
  2. F

ANSWER: A

What are some very common ways of compromising Apple computers these days?

* 1. Installing software that is unapproved by your IT and Security teams
  2. Fake Flash Player updates
  3. Fake antivirus installs
  4. Fake browser updates
  5. All of the above

ANSWER: E

What should you always make sure is turned on in your Mac computer’s settings?

* 1. Your operating system is being auto-updated
  2. Your alarm settings cannot be overridden
  3. Your operating system and all apps are being auto-updated
  4. None of the above

ANSWER: C

If you are a frequent traveler, it is strongly suggested that you set up FileVault on your Apple laptop so that your hard drive contents are encrypted:

* 1. T
  2. F

ANSWER: A

Why should you periodically review the Privacy tab in your Apple’s Security settings?

* 1. To check any specific permissions that your installed apps are asking to use
  2. To see who is sitting in the same coffee shop as you, and is snooping on you
  3. To make sure your computer is invisible to the Internet
  4. None of the above

ANSWER: A

Smartphones and Mobile Apps

Android has a number of security issues such as:

* 1. An open app development platform that makes it easier to upload an app into the Google Play Store
  2. Most malicious apps are developed for Android phones
  3. Many mobile manufacturers do not push out timely Android security updates
  4. Many Android apps are not set to update automatically
  5. Most Android phones are running an older operating system
  6. All of the above

ANSWER: F

Never install any Android apps from anywhere outside of the Google Play Store:

* 1. T
  2. F

ANSWER: A

Consider downloading a new mobile app from an app store the same way you would consider buying something off eBay:

* 1. T
  2. F

ANSWER: A

If you install a malicious app, it will usually send texts to premium rate numbers, steal your passwords, or intercept your phone calls and text messages:

1. T
2. F

ANSWER: T

What should you consider before downloading any app from an App Store?

1. How many apps does the app developer have?
2. What kinds of reviews does the app have?
3. How many reviews does the app have?
4. What are the permissions the app needs to run?
5. All of the above

ANSWER: E

What are some tell-tale signs an app may be malicious?

1. It looks very similar to a popular legitimate app
2. It will ask for excessive permissions once you have installed the app
3. It asks for permissions to access your SMS text messages
4. It is hosted on a third-party app store on the Internet
5. All of the above

ANSWER: E

iPhone is generally a more secure mobile device, because there are very few malicious apps in the App Store, and because Apple will keep pestering you until you install the latest operating system:

* 1. T
  2. F

ANSWER: A

A very important security setting you should turn on in your mobile device is:

* 1. The read-only settings in the browser
  2. Auto-updating the operating system and all installed apps
  3. The email forwarding feature in the email client
  4. None of the above

ANSWER: B

Always review each mobile app for the permissions it uses, to make sure nothing suspicious stands out:

* 1. T
  2. F

ANSWER: A

What are some tell-tale signs that you have actually installed a malicious app?

* 1. Your battery is suddenly draining quickly
  2. You suddenly start experiencing many dropped calls
  3. You notice excessive app data usage on your monthly bill
  4. All of the above

ANSWER: D

What should you do if you think you may have installed something malicious on your mobile device?

* 1. Stop using it, especially to connect to sites such as banking and email. Best thing to do is turn it off
  2. If it’s a personal phone, wipe the phone using a full factory reset
  3. If it’s a work phone, immediately talk to your IT Security department
  4. Send it in to the phone manufacturer for a refund
  5. A, B and C

ANSWER: E

What are two very important security features you are strongly urged to set up today?

* 1. Turn on FindMyPhone/FindMyDroid
  2. Set up an 8-character PIN
  3. A & B
  4. None of the above

ANSWER: C

Password Management

What is the number one issue when it comes to using passwords?

* 1. We use the same, weak password across different websites
  2. Our passwords cannot be carried around like a mobile device
  3. We like to write them in our journals
  4. Passwords are not really necessary

ANSWER: A

What is most important attribute in a strong password?

* 1. It should be complex, meaning it should have special characters and numbers
  2. It should be posted on your computer monitor
  3. It should be long, preferably 16 characters or more
  4. It should be shared with colleagues for the sake of convenience

ANSWER: C

A memorable catchphrase, from a song or movie, is a great example to use, to create a base password:

* 1. T
  2. F

ANSWER: A

Why is a password manager so useful for managing all of our passwords?

* 1. It can easily store thousands of them in a very secure vault
  2. It can be configured to recommend as many 16-character complex passwords as you need for every website you log into
  3. It is easy to set up and can be synced across devices
  4. Its password vault can be protected with a master password that only you know
  5. All of the above

ANSWER: E

2FA

At a basic level, 2FA works by enforcing a second factor (something you have in your possession) in addition to the first factor (something you know, such as your username and password):

* 1. T
  2. F

ANSWER: A

The best thing about 2FA is it protects your account, especially if you decide to use a weak password:

* 1. T
  2. F

ANSWER: A

Hackers HATE 2FA, as it prevents them from hijacking your accounts for this reason:

* 1. The hacker has to be able to steal your credentials
  2. The hacker has to have physical possession of your mobile phone
  3. The hacker has to know the PIN to access your mobile phone
  4. All of the above

ANSWER: D

The best form of 2FA to use is:

* 1. Authentication app
  2. SMS text-based
  3. Physical security key
  4. None of the above

ANSWER: C

Yubikey and Google Titan are two security keys that are easy to set up and use when logging into some popular websites:

* 1. T
  2. F

ANSWER: A

Browser Security

Which of these are true about trackers?

* 1. They are browser scripts that profile who you are, and what you like, for marketing purposes
  2. They can increase the load time of the average webpage by 50%
  3. There can be many different trackers running at the same time on popular websites
  4. They can be used to uniquely fingerprint your browser
  5. All of the above

ANSWER: E

Javascript is extremely useful for making all of the websites on the Internet more dynamic and entertaining, but there are also many malicious Javascripts that run on certain websites:

* 1. T
  2. F

ANSWER: A

Scripts can be used for:

* 1. Advertisements
  2. Trackers
  3. Cryptominers
  4. Browser fingerprinting
  5. All of the above

ANSWER: E

Add-ons like NoScript show you all the extra scripts running on a website so you can selectively allow/deny them from running?

* 1. T
  2. F

ANSWER: A

What are some problems when it comes to browsers:

* 1. Malicious scripts
  2. Trackers and third-party cookies
  3. Fake Flash Player messages
  4. Fake versions of popular extensions and add-ons
  5. Fake browser updates
  6. All of the above

ANSWER: F

What are some security measures you should absolutely take to lock down your browser?

* 1. Set your browser to auto-update
  2. Set all your add-ons and extensions to auto-update
  3. Delete Flash and Java plugins
  4. Review and delete any add-ons, extensions and plugins you don’t truly need
  5. Set your Flash plugin to “Ask to Activate”?
  6. All of the above

ANSWER: F

Chrome is a secure browser to use, but it can become very insecure if you install malicious extensions:

* 1. T
  2. F

ANSWER: A

1st-party cookies are generally good, whereas 3rd-party cookies are normally placed by websites you didn’t even intend to visit, so that they can track your browsing habits:

* 1. T
  2. F

ANSWER: A

What is true about seeing “HTTPS” in your browser address bar?

* 1. HTTPS means the website itself is very safe to visit
  2. HTTPS means the connection between you and the website is encrypted inside a secure tunnel
  3. HTTPS means you can freely hand over all your personal data to the site
  4. None of the above

ANSWER: B

Social Media

Always be careful NOT to post sensitive personal or company data on social media?

* 1. T
  2. F

ANSWER: A

Hackers and fraudsters love social media platforms because:

* 1. They are perfect for sharing links, articles, pictures and videos with large numbers of people at a time
  2. There are over 1 billion people using social media these days
  3. Its relatively easy to create catchy and intriguing posts that can social engineer people into clicking on them
  4. All of the above

ANSWER: D

Never trust any posted content, even if it was supposedly posted by your trusted friend:

* 1. T
  2. F

ANSWER: A

Catch phrases such as “Check this out!” “Wow!” and “OMG!” would never ever lead to malicious or fraudulent posts:

* 1. T
  2. F

ANSWER: B

Disinformation

Research shows that false news travels 70% faster than real news across the Internet:

* 1. T
  2. F

ANSWER: A

What makes false news/disinformation content so viral?

* 1. It is cutting edge
  2. It is interesting
  3. It might align with our pre-existing beliefs
  4. All of the above

ANSWER: D

Why is false news/disinformation so dangerous from a cyber security perspective?

* 1. Anyone today can be a content creator, and secretly post malicious content which then goes viral on social media
  2. Sources of false news can just as easily be sources of malicious webpages and content
  3. There is very little editorial oversight for posted social media content, so malicious content can be posted without many checks and balances
  4. All of the above

ANSWER: D

It is crucial for all of us to be critical thinkers when we see any posted content on social media:

* 1. T
  2. F

ANSWER: A

Internet Data Privacy

If you log into a website offering free services on the Internet, it should be assumed that:

* 1. The services are free with no strings attached whatsoever
  2. The website will monitor your web traffic and interests, so they can monetize your data in the form of targeted ads
  3. You will always receive the services for free
  4. All of the above

ANSWER: B

What are some good ways to prevent your data from being monetized without your knowledge on the Internet?

* 1. Use Facebook, Google and Twitter credentials on as many login pages as you can, as a matter of convenience
  2. Use a browser such as Brave or Firefox which blocks trackers by default
  3. Always create a separate and unique username/password for each new website in which you create an account
  4. Go into websites such as Facebook and Google, and review and/or delete the data they have about you
  5. B, C and D

ANSWER: E

If you’re using a service for free on the Internet, you might not be the customer, but the product being sold:

* 1. T
  2. F

ANSWER: A

Identity Theft

Because of all the major breaches in recent years, we should all assume our private and sensitive data could already be in the hands of the bad guys:

* 1. T
  2. F

ANSWER: A

Which one of these is true for a Credit Freeze:

* 1. It acts like 2FA for your credit profile
  2. No one can ever pull your credit report unless you ‘UNFREEZE’ your account
  3. It is completely free
  4. No one can take out any loans or mortgages in your name unless you ‘UNFREEZE’ your account
  5. All of the above

ANSWER: E

You should set up a Credit FREEZE (not Credit Lock) and Fraud Alert as soon as possible:

* 1. T
  2. F

ANSWER: A

GDPR

GDPR helps protect the privacy of your client data, by enforcing strict privacy controls around the data:

* 1. T
  2. F

ANSWER: A

If you are providing services to European citizens, you have to:

* 1. Be very explicit about what private data you are using
  2. Explain why you are using the client’s data
  3. State for how long you will be using that data
  4. Provide your client with the option to review and/or delete their data
  5. All of the above

ANSWER: E

What is one VERY important security control you should implement, to protect your company from hackers, and subsequent GDPR sanctions?

* 1. Sign up for GDPR notifications
  2. Encrypt all sensitive customer/client data
  3. Make sure your company is registered in Europe
  4. Make sure your manager is notified if you are not a European citizen
  5. None of the above

ANSWER: B

Encryption/Travel

It is important that you always ask your manager, IT or IT Security team for help or guidance if you need to install any encryption software to protect sensitive customer/client data:

* 1. T
  2. F

ANSWER: A

What are some things you can encrypt to make sure your clients data stays private and secure?

* 1. Text messaging
  2. Hard drive
  3. Web traffic to your cloud app
  4. Files and folders
  5. Emails
  6. All of the above

ANSWER: F

When you see HTTPS in your browser address bar right before the website address, it means:

* 1. You web traffic is encrypted, so it cannot be intercepted and read by anyone
  2. Your browser is a new version and doesn’t need updating
  3. Your web traffic is optimized for speed and accuracy
  4. None of the above

ANSWER: A

iMessage, WhatsApp, and Signal are messaging apps that maintain a truly encrypted message between you and the person you are messaging:

* 1. T
  2. F

ANSWER: A

When traveling, what are some things you can use to keep your web traffic and sensitive data secure?

* 1. Only use apps and software that have been approved by your IT Department
  2. Only travel with the minimal amount of company data to do your job
  3. Always encrypt everything you can
  4. All of the above

ANSWER: D

IoT Internet of Things

Which one of these are what we call IoT devices?

* 1. Internet-connected fridge
  2. “Smart” TV
  3. Pacemaker
  4. Home router
  5. Internet-connected toaster
  6. All of the above

ANSWER: F

What are the main security issues with IoT?

* 1. Most IoT devices do not have any auto-update features
  2. The manufacturers rush them to market with little security built in
  3. Their default usernames/passwords are weak and well known
  4. Because they usually have no screens, they are hard to manage
  5. They usually ship with insecure default settings like remote management turned on
  6. All of the above

ANSWER: F

What is the best way to manage any IoT device you own?

* 1. The same way you would manage a regular computer
  2. Like an expensive gift
  3. Like you would manage traffic on a busy freeway
  4. Similar to how you would manage yourself

ANSWER: A

Nation states hackers are breaking into thousands of our home IoT devices, so that they can be used to attack Internet websites:

* 1. T
  2. F

ANSWER: A

What are some things you should do when you bring a new router into your home?

* 1. Change the default password to a random one that is 16 characters or more
  2. Disable any remote management features such as uPnP
  3. Update the firmware
  4. Change the network name (SSID)
  5. Set up the strongest Wi-Fi encryption using WPA2 – PSK
  6. All of the above

ANSWER: F

What Else Can You Do To Protect Yourself?

Anytime you receive an email, text, or phone call at work or at home, you should:

* 1. Pause
  2. Check your emotions
  3. Notice any red flags
  4. Avoid clicking any embedded links unless you’re 100% certain it’s safe
  5. Avoid downloading attachments unless you’re 100% certain it’s safe
  6. All of the above

ANSWER: F

What is one of the THE most important things to remember in this entire training series?

1. Hover your mouse over links in emails to see where the link actually takes you
2. A
3. Definitely A
4. Most certainly A
5. All of the above

ANSWER: E

On the Internet, never trust anyone you don’t know, but friends, family and colleagues are 100% to be trusted:

1. T
2. F

ANSWER: B

Never leave your laptop unattended at work, unless it is locked away in a secure location?

1. T
2. F

ANSWER: A

Keep your browsing to a minimum and only to very well-known legitimate websites whilst at work:

1. T
2. F

ANSWER: A

Don’t bother auto-updating your operating system, browser, add-ons, extensions, and applications because the chances of a hacker wanting to break into your computer or accounts is slim at best:

1. T
2. F

ANSWER: B

Make a habit of installing UNAPPROVED applications, mobile apps, browser add-ons, extensions and plugins on your devices. It helps stop a hacker from breaking into your network?

A. T

1. F

ANSWER: B

Definitely DO NOT install a password manager to manage all of your hundreds of passwords, and definitely DO NOT make any of your passphrases/passwords 16 characters in length:

1. T
2. F

ANSWER: B

Make sure you carefully back up all of client’s sensitive data to only company-approved Cloud apps and external drives?

1. T
2. F

ANSWER: A

Having an ‘next-generation’ antivirus program on your system:

1. Is fantastic, and helps stop many types of malware from taking over your system
2. Will make you 100% secure forever and ever
3. Is extremely important to keep up-to-date and scanning all your files often
4. Is even better if it has artificial intelligence and machine learning built in
5. A, C and D

ANSWER: E