
CYBER SECURITY
AWARENESS

WHAT'S ALL THIS "CYBER" STUFF ANYWAY?

Cyber (Security) Awareness

It's not just knowledge; security awareness is knowledge combined with attitudes and behaviors that serve to protect our information assets. Being aware means you understand what threats are and how to take the right steps to prevent them.

Cyber Security

The body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Cyber Defense

Focuses on preventing, detecting, and providing timely responses to attacks or threats so that no infrastructure or information is tampered with.


DEFINITIONS

BACKDOOR

A backdoor in a computer system is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

CLICK-JACKING

A malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page owned by someone else.

DENIAL-OF-SERVICE ATTACK (DOS)

Designed to make a machine or network resource unavailable to its intended users. An example would be deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

DIRECT-ACCESS ATTACK

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making modifications, installing software worms, keyloggers, covert listening devices, or using wireless mice.

EAVESDROPPING

A form of the "Man in the Middle" attack. The act of surreptitiously listening to a private conversation, typically between hosts on a network.

PHISHING

The attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trust, phishing can be classified as a form of social engineering.

SOCIAL ENGINEERING

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer. A common scam involves fake CEO emails sent to accounting and finance departments.

SPOOFING

In general, spoofing is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

TAMPERING

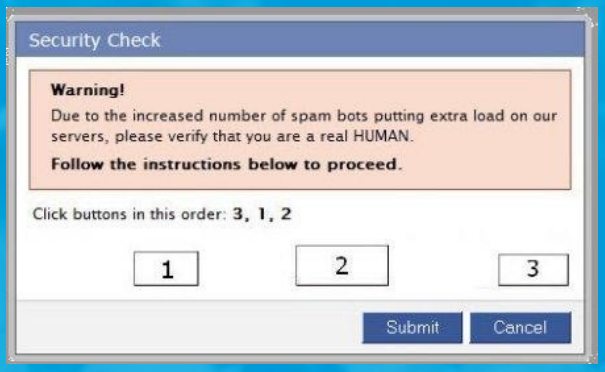
A malicious modification of products with the intent to disrupt established rules or protocols, such as installing a keylogging device or removing or replacing network cables.

Common Attacks and How To Watch Out For Them

Click-jacking

This example references Facebook; it could easily come from any web page...

When you see a post on a Facebook friend's wall that seems out of character, don't be too quick to click. That post labeled “Pictures of Cute Cats” or “Best All-Time Fails” could be a click-jacking attack. This type of attack isn’t always malicious, but it can definitely be annoying. Usually the post itself uses a short phrase or sentence that's just a bit provocative. The point is to arouse your curiosity. A common method is to make you “prove” you’re old enough to see the material. You may get a warning such as this one on the left:



Once you click the button to confirm your age you may see another embedded dialog box, as shown by the example on the right. This one claims a need to prove that you're “human” in order to avoid spam bots that are "putting an extra load on our servers." This part may ask that you click numbered buttons in a certain order, like this:

Clicking those buttons doesn't prove anything, and in fact may mean that you’re now posting the click-jacking attack in your own Facebook profile, thereby spreading it to all of your friends. If you encounter this type of attack, resist the urge to click the buttons. There are legitimate reasons for having to prove yourself, but just be aware that not all may be beneficial – think about what you’re trying to do, whether or not you’re on a “real” web page or just something that “popped up.”

These factors could make the difference between getting what you want or posting naked celebrity pictures to your mom’s Facebook page!

Direct-Access Attack

A direct-access attack can be one of the most highly destructive forms of attack, yet can also be one of the easiest to prevent.

If an attacker is able to gain access to a computer that they normally wouldn't be able to, they could possibly download data from it. They can also compromise security by modifying installed software or add hardware that would attempt to break existing security methods.

If an attacker is able to gain unauthorized access to a secure room (such as a server room, network closet, phone room, etc.), then the possible damage level is increased tremendously.

Every contractor, visitor, vendor, or guest to a Baker College campus should have some form of ID badge visible on their person. A simple "may I help you" may mean the difference between a security breach and someone just looking for a classroom.

Someone is hanging around in an office that belongs to someone else, you see someone walk out of a secure area without an ID, individuals that you know aren't the local IT or Facilities personnel are working in an electrical room or a phone closet – these are all examples of potential direct-access attacks. If you don't feel comfortable asking for ID or proof of why they're here, then get Campus Safety involved to ensure everyone is accounted for.

If the entire campus acted as "one" set of eyes, a direct-access attack would be almost impossible to pull off. Be aware!

Easily one of the most common attacks, the "phishing" attack simply tries to get you to give out personal information of your own free will – and to some extent, they almost always work.

Learn to Identify Suspected Phishing eMails

- They often duplicate the image of a real company.
- Sensational messages such as "Urgent! Your Action is Required!"
- Use real company names or actual employee names.
- Use logos that appear "correct" or very similar to the actual company logo.
- Grammar/Punctuation is slightly off (misspelled words, no commas, etc.)

Watch Those Links!

Check any hyperlink or "click here" button. Hover your mouse over the link or button, but **DO NOT CLICK** on them. Look for link address to pop up or show up in your browser window (usually at the bottom left). If you see an address such as "http://tinyurl.com/AA20zh" or some random web page, this is a great clue that the link will lead to nothing but trouble. Be careful here, however; if your normal bank web page is (for example) "www.bankofamerica.com", the phishing version could show up as "www.bankoftheamericas.com". Close, but just not right!

(continued…)

Enter Your Sensitive Data in Secure Websites Only

In order for a site to be ‘safe’, it must begin with ‘https://’ and your browser should show an icon of a closed lock, usually up by the web page address. If you don’t see either of these items, use EXTREME caution if you decide to proceed any further. Your best bet at this point would be to call the company directly to handle your transaction or at least to verify if you’re on the right web page or not. After all, you’ve got nothing to lose but your ENTIRE LIFE SAVINGS, right?

Phishing Doesn’t Only Pertain to Online Banking

Most phishing attacks are against banks, but can also use any popular website to steal personal data such as eBay, Facebook, PayPal, etc.

Phishing Knows All Languages

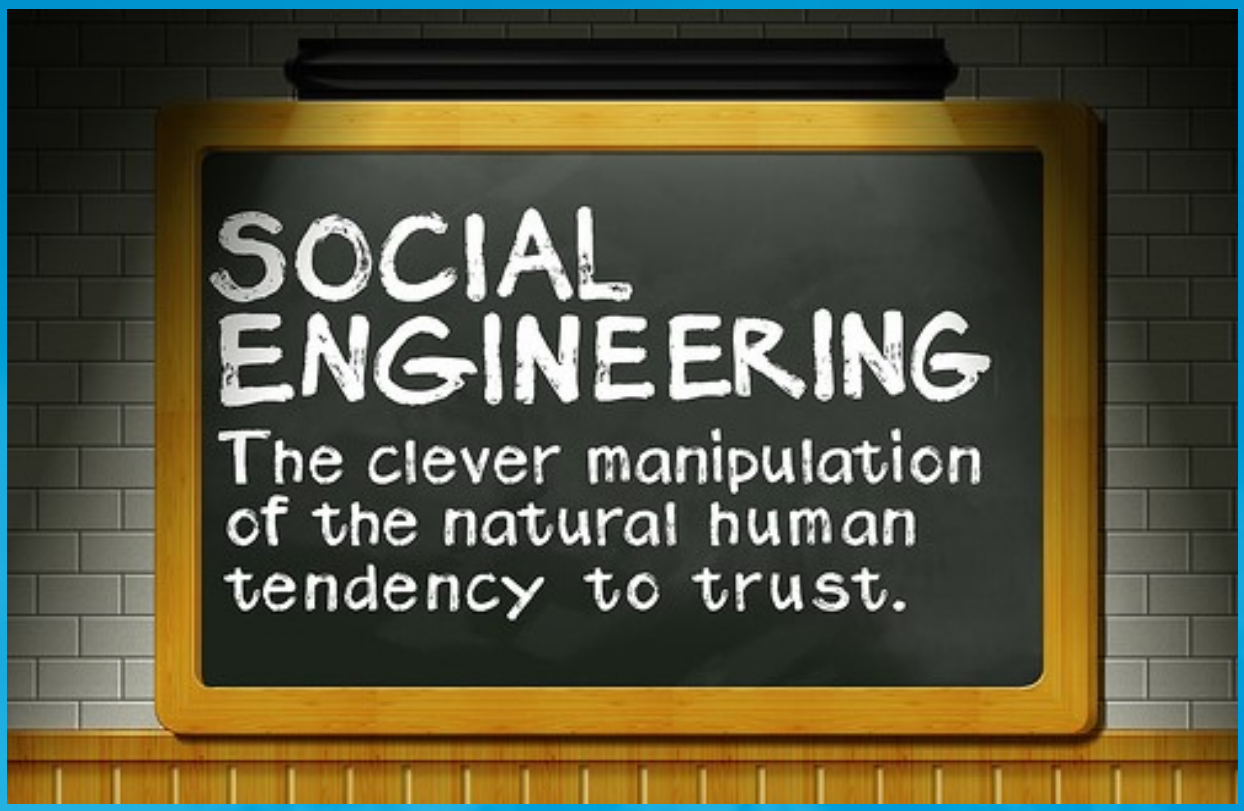
Phishing knows no boundaries, and can reach you in any language. In general, they’re poorly written or translated, so this may be another indicator that something is wrong. If you never you go to the Spanish website of your bank, why should your statements now be in this language?

Have the Slightest Doubt, Do Not Risk It

The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data.

Toughen Up!

Don't get pressured into providing sensitive information. Phishers like to use scare tactics, and may threaten to disable an account or delay services until you update certain information. Be sure to contact the merchant directly to confirm the authenticity of their request.



In a social engineering attack, an attacker uses human interaction (social skills) to obtain information about an organization or its computer systems. An attacker may seem respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility (for example, "Hi, Joe. Mary over in Academics said I should talk to you about some info I need").

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving up a password than it is to try and hack the password (unless it's a really weak one).

Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on your doors and windows, or if you have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if you trust the person at the gate who says he's the pizza delivery guy and you let him in without first checking to see if he is legitimate you are completely exposed to whatever risk he represents.

(continued)...

Common Social Engineering Attacks
(note that "Phishing" is a form of Social Engineering)

Emails from a friend that contain a link that *you just have to check out* – and because the link comes from a friend and you're curious, you'll trust the link and click – and be infected with malware so the criminal can take over your machine and collect your contact info and deceive them just as you were.

Messages that contain a download (pictures, music, documents, etc.) that has malicious software embedded. If you download – which you are likely to do since you think it's from your friend, you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know. And on, and on.

An urgent plea for help – your "friend" is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.

Someone asks you to donate to their charitable fundraiser (or some other cause) – with instructions on how to send the money to the criminal.

A message may notify you that you're a "winner." Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your winnings you have to provide *information about your bank routing* so they know how to send it to you, or give your address and phone number so they can send the prize, and you may also be asked to *prove who you are by* often including your Social Security Number.

Baiting scenarios. These schemes know that if you dangle something people want, many people will take the bait. These schemes are often found on Peer-to-Peer sites offering a download of something like a hot new movie, or music. But the schemes are also found on social networking sites, malicious websites you find through search results, and so on.

Auction schemes – These show up as amazing deals on classified sites, auction sites, etc. To allay your suspicion, you can see the seller has a good rating (all planned and crafted ahead of time). People who take the bait may be infected with malicious software that can generate any number of new exploits against themselves and their contacts, may lose their money without receiving their purchased item, and, if they were foolish enough to pay with a check, may find their bank account empty.

There are endless variations to social engineering attacks. The only limit to the number of ways they can socially engineer users through this kind of exploit is the criminal's imagination. You also may experience multiple forms of exploits in a single attack. Then the criminal is likely to sell your information to others so they too can run their exploits against you, your friends, your friends' friends, and so on as criminals leverage people's misplaced trust.

Spoofing

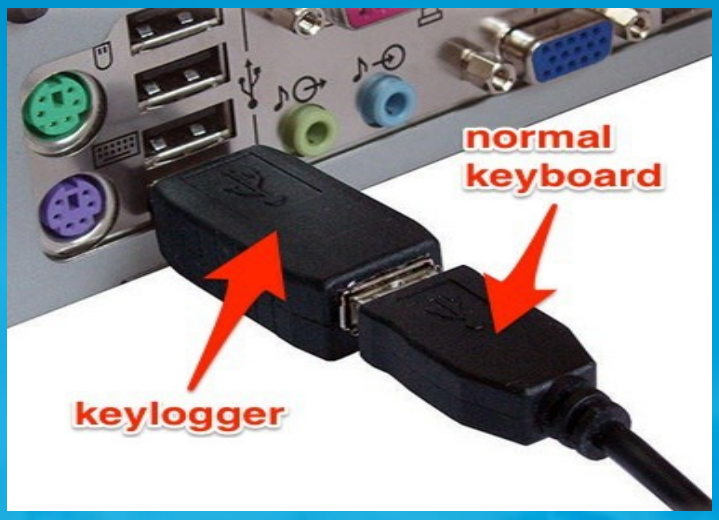
A “Spoofer” knows that if a recipient receives a spoof that appears to be from a known source (such as your credit card company), it is likely to be opened and acted upon. Spoofing differs from Phishing in that a spoof is a pixel-perfect representation of a merchant or company. The quality of workmanship is far better than a typical phishing attempt in that it might even fool an experienced security professional.

Herein lies the premise of spoofing; an official-looking correspondence from an important service provider instructs you to take precautionary actions to protect your finances or reputation. Corporate logos and other distinctive graphics are easy for hackers to hijack and embed in emails or other documents. These professional graphic elements convince end-users that an impending threat can be suppressed by following the sender’s instructions, which usually entails clicking on a link of some sort. In most cases the link executes a malicious file that damages your operating system and critical applications while it propagates throughout your network, placing other clients and vendors at risk.

Caller ID spoofing is the process of changing the caller ID to any number other than the calling number. When a phone receives a call, the caller ID is transmitted between the first and second ring of the phone. Spoofers will often use available systems to “change” or “spoof” the outgoing number so that it represents an actual number that belongs to a bank, credit card company, insurance agency, etc. If you see a number you recognize, you’re more likely to answer the call and be fooled into providing information that you normally wouldn’t (to someone calling from an unknown phone number, for example).

Again, prevention comes in the form of knowledge. Be aware of your online presence. Avoid being careless and take the time to assess your surroundings when the time comes. If you receive an email from your corporate headquarters, make sure every detail looks correct. Even if it does, ask yourself WHY am I getting this email – does it seem like something I would be singled out for? Don’t be afraid to call the sender and ask if they actually sent the email. Answer a phone with the intent of helping the caller but without providing sensitive information such as network details, types of equipment in your organization, or non-public directory information. Keep it safe!

TAMPERING



Have you ever seen anyone working "behind" a computer that normally wouldn't be there? Someone sitting in front of a computer in an office that's not theirs? A computer's network cable unplugged and left disconnected? These are all examples of possible tampering.

Let's say you have a student in your office and you have to step out for a moment to retrieve a print job. While you're out, the student quickly detaches your keyboard from your computer and plugs the cable into a "key logger" device and then plugs it back into the computer. The entire time that key logger is in place, it is recording your every keystroke, passwords and other secrets alike. Then, the student makes another "appointment" with you and when they're in your office, they quickly retrieve the key logger just as easily as they put it there in the first place. They review the key logger's log file and learn all the passwords you've typed in for your bank, your credit cards, your job, and your CVS prescription account. Feel violated? You should.

You walk by a classroom or an office and notice someone with a laptop sitting at a desk that already has a computer. You look a little closer and notice that the network cable from the existing computer is gone, and that it looks like it's plugged into the "visitor's" laptop. This could quite easily be someone trying to hack into the network environment and probe for weaknesses that could be exploited later. This could also be someone who already discovered a weakness from a prior hack and is now attempting to disrupt or abuse information now available to them. Thousands of social security numbers, personal information, or credit card information could be now sold to the highest bidder and create chaos for countless innocent victims.

These are not TV or movie scenarios – they happen in real life and happen often. Sony, Chase Bank, Target, British Airways, eBay, UPS, and even the IRS have been victims of data security breaches, along with countless others. How can you make a difference? Be aware of your surroundings and what seems "normal." As you go about your daily activities, be conscious of activities around you and if something seems out of place don't be afraid to question. Your one question could save hundreds or thousands of people from becoming victims. It's that simple!


Best
Practices

Your Dog's Name Is Not a Password

Try using a phrase that you'll remember, such as -
"My Dog Likes to Sleep by the Kitchen Door"
Use every first letter and replace some with numbers or symbols -
MdL7$8+kd

Beware of IRS or phony computer support scams.

Shut down or restart your computer at least weekly.

Don't open unsolicited or unexpected attachments.

Don't open emails from unrecognized senders!

Secure laptops and mobile devices at all times!

Educate yourself—visit the Baker IT web page for more help.

Only click on links from trusted sources!

Don't log into web sites unless the login page is secure.

Make backup copies of files or data you are not willing to lose!

Limit your web browsing to work-related sites as much as possible.

Report any suspicious use to Campus Safety or your local IT Department.

Shut down, lock, or log off your computer before leaving it unattended.


Need More Info?
http://www.baker.edu/security


VIRUS
INTRUDER
How aware
are YOU ?

Baker College

Baker College will never ask for your account password.

(we already have your password)

Any communication that asks for your account password is a scam.
Please contact the Baker College ITSC at
800-645-8350 / 810-766-4060
if you have any questions.