Acceptable Use Cheat Sheet:

For more detailed Acceptable Use information, check out the Acceptable Use Policy.

When in the Office:

- Use caution when opening emails you weren't expecting.
- Use caution when opening attachments or following links in emails you weren't expecting.
- Do not write down your passwords.
- Do not store sensitive information on your desk.
- Report or challenge suspicious activities/people/situations.
- Lock your laptop when you leave your desk (Command + Control + Q on the Mac)
- Wear your badge.
- Don't install personal equipment (switches, etc) in the office.
- Don't throw or otherwise damage your computer…or your co workers.
- Don't leave stuff on Printers, please use the shred bins instead if you need to get rid of something you printed.

When Remote:

- Keep an eye on your stuff, don't let it walk off!
- Don't let someone else use it.
- Don't throw or otherwise damage your computer…or other people.
- Don't download or store files on your personal computers or other devices.
- Remember that any data you download, you're responsible for keeping safe.
- Don't leave it in your car.

Never:

- Use company owned equipment for…"questionable" stuff (adult content, software piracy, sending spam, working another job, etc.).
- Store any illegal content or data on company equipment.
- Use your company equipment to break Copyright Laws.
- Autoforward your work email to personal email accounts.
- Be an unprofessional jerk to your coworkers.
- Use anonymizers and other proxy services with company equipment (TOR).
- Use a personal email address for company business, its confusing and one of the easiest ways companies get hacked and defrauded!
- Upload company data to your Cloud provider (Github, iCloud, etc)
- Mess with, tamper, or break company gear…or people.

Am I being monitored?

If you're on your work laptop, using company data, or in the office, the short answer is yes.

What's being monitored?

We mostly monitor for things that could potentially put the company, our reputation, our customers, Partners, or Employees at risk. This includes, but isn't limited to:

- Where our data is going (who, what, where, etc)
- Is it all legal?
- Can it cause us to be sued?
- Can it cause us harm either in terms of money or reputation?
- Can it disrupt operations?
- Does it put the building, our co workers, or our business in danger?
- Does it constitute theft of company Intellectual Property or gear?

Data Classification & Handling Cheat Sheet:

For more detailed classification & handling information, check out the Data Classification and Data Handling Policies.

Class 1-Highly Confidential:
Data only accessed with a critical business need to know, whose disclosure could cause direct or indirect harm to corporate interests or legal standing.

Examples:

- Payment and/or Financial Account Information such as:
  - logins and passwords
  - account numbers
  - PayPal and Venmo information
  - Tokens
  - Backend API Keys
- ANY Personal Information for any individual, such as:
  - Social Security & License Numbers
  - Names and Birthdates
  - Shopping and Browsing History
  - Addresses, Geo Data, IP Data
  - Marital Status
  - Household Income
  - Loyalty Card info
  - Email and Social Media User Info
  - Device and other Identifiers (UDID, MAID, IDFA, IDFV)
  - Medical data such as:
    - Health Insurance
    - HSA/FSA data
    - Prescription Information
    - Birth and Death certificates
  - Biometric Information such as:
    - Fingerprints, voice prints
- Legal information such as:
  - Litigation Information
  - Intellectual Property
  - Trade Secrets

Handling Class 1 Data:

- Do not Disclose/send outside Company without security review and NDAs and Contracts in place.
- Do not send via Email or Electronic Messaging.
- Minimal Access on business need to know.
- Do not store locally.
- Do not store on Removable Media.

Class 2-Confidential:
Data only accessed with a business need to know, whose disclosure could compromise corporate interests.

Examples:

- Product Strategies, Source Code, Network Diagrams, Corporate Financial Ledgers.
- Deidentified/Aggregate Consumer Data
- Company Examples:
  - Product/Marketing Strategies.
  - Business Trends
  - WiFi Passwords
  - Contract Details
  - Business Plans
  - Financial Models & Projections
  - Customer IDs
  - Analytics
  - B2B Data
  - Machine Learning & Data Engineering Project Code
  - Proprietary Algorithms, Technology & Source Code
  - Manufacturing & Product Specifications
  - Database Tables & Schema

Handling Class 2 Data:

- Disclosure & Access on business need to know.
- Send outside only with valid business need to know, and contracts and NDAs in place.
- Can only be stored on Company owned and managed devices & services.
- Can only be shared after vendor passes security review.

Have a question?
Reach out to either Management or Security and we'll be happy to help answer them.

Class 3-Public:
Data anyone can view.

Examples:

- Case Studies
- Open Source Code Reviewed/ Tested for Security Concerns
- Blog Posts
- Headquarters Address
- Main Phone Number
- Information on the Company public internet site
- Privacy Policy

Handling Class 3 Data:

- No access limitations.
- No storage requirements.
- No sending requirements.

Definitions:

Deidentified Data:
is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

Aggregate Data:
Relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linked to any consumer or household, including via a device.

Phishing & Scams Cheat Sheet:

Phishing/Vishing/Smishing Oh my!

Phishing: Using email to con a victim into either revealing sensitive information (like a password) or installing malware.

- **Spear Phishing**: Targeted phishing to a specific victim or group of victims (like a specific attempt to con Marketing)
- **Whaling**: Targeted phishing to a specific executive at an organization.

Vishing: Using voice (like a phone call or Skype call) to con a victim.
Smishing: Using SMS/Text messaging to con a victim.

What do I look for? (Phishing)

Phishing emails generally:

- Have grammatical errors.
- Are not personalized at all (Dear Customer).
- Use scare tactics (the IRS has your information and will file lawsuits).
- The sender name and domain name spoof a known brand.

Will attach files that embed malicious code (like office macros) to run on and infect your computer when the file is ran. Do not click to enable Macros (or Content, depending on the Office version) on a document you weren't expecting, or from someone you don't know.

Spoofed Links: Always hover over any link before you click on it, if the link itself doesn't match the website you think it should, be careful!

Spoofed websites: will use links that basically provide a duplicate of a legit website, only the URL will be something like "www.bankofannerica.com" instead of "www.bankofamerica.com"

What do I look for? (Vishing)

- Usually uses scare tactics (posing as an IRS agent, posing as "tech support" or "Microsoft/Apple".
- Anything that requires immediate action is almost guaranteed to be a scam.
- The IRS, Apple, Microsoft, etc. are NEVER going to call you out of the blue about your "social security number being used for fraud" or "we have detected a virus on your laptop" (they say laptop because they will be right more often than not anymore, same reason they usually say 'windows laptop' specifically).

What do I look for? (Smishing)

- Masked phone numbers,
- Spoofed websites impersonating a brand,
- Messages that come from out of thin air,
- May use the first or last few numbers of a known account (especially if it was tied to a previous hack) to try and pressure you into responding.

Password Reset cons

Smishers have spoofed two factor authentication for a number of services, here's how they do it:

- Attacker gets victim's email/phone from other sources (usually public info)
- Attacker poses as victim and asks company (we'll say Google) for a password reset.
- Google sends a text reset code to victim without the victim asking for it (because they didn't, the attacker did).
- Attacker sends the victim a text message similar to this: "Google has detected unusual activity on your account. Please respond with the code sent to your mobile device immediately."
- The victim sends the verification code to the attacker thinking the request came from Google.
- Attacker users the code to reset the victim's password, take control of their account, and profit.

Don't respond or act on unsolicited text messages. If you didn't ask for it, delete it!

Spears and Whales?

Spear phishing and whaling are both normally far more personalized, and will "name drop" if possible.

Universal Signs its a Scam

These tips can be applied to pretty much any situation, online, via letters, in person.

- If it seems too good to be true or sounds at all questionable, it probably is.
- Always be suspicious of unsolicited communications.
- Don't click on links or attachments if it looks at all questionable.
- Directly contact the purported sender via "known" legitimate and good channels.

Zoom/Online meeting scams

Online meeting/messaging platforms like Zoom/Slack aren't immune to this, either. Here are some things to watch out for:

- Unsolicited meeting invites (if you don't know them, don't accept it)
- Screen sharing requests
- Any remote support requests you didn't ask for, especially ones that don't come from IT

So I think I got sent a scam, now what?

If you get something that appears suspicious, and especially if it claims to be from someone you know or a company you work with, you can follow these steps to confirm if its legit:

Contact the sender via a different method:
Say you get an email from your "bank"and it has a link that looks shady. Instead of clicking on the link itself, go directly to your bank's website or app that you've used before, and login that way to check. Or call. Get a text from a number you don't know or email from your manager from a different address wanting you to buy a bunch of gift cards you'll get reimbursed for? Call them to confirm it, or email them through their Company email address.

Report it as phishing:
If its coming to your Company email address, report suspicious emails and we'll take a look at it. This also allows us to correlate phishing campaigns that are sent to multiple employees, as well as other organizations we get threat information from about potential attacks and other shady scams floating around the net. If its found to be malicious, we (security) will delete the email from your (and everyone else who got it)'s mailboxes.

Random Fact (Phishing through the Ages)

One of the most popular scam emails in the modern world is called the "Nigerian Prince" due to the fact that the first couple of thousand of these found in the wild mentioned a Nigerian Prince in need of help (which is funny given that Nigeria is a Republic and therefore has no royalty) but it still works, to the tune of over $700,000 scammed out of people in 2019. It's a variant of a centuries old scam called the "adance-free scam" the most famous example is the "Spanish Prisoner" from the 18th and 19th Century. What all of these share is basically how they work, which is like this:

The scammer contacts the victim, claiming someone important (the Prince, or Prisoner) requires help getting access to a large sum of money to get released from prison or whatever, and only the victim (amazing person they are) can help! How? By giving the scammer a small sum of money to help the someone important get out, and when the someone important gets out, they will send a LARGE SUM OF MONEY as a thank you for being awesome and helping them make bail. The scammer, of course, just takes the money and runs.