

# CYBER SECURITY AWARENESS WORKSHOP



Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information.

Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Many large enterprises employ a dedicated security group to implement and maintain the organization's infosec program. Typically, this group is led by a chief information security officer. The security group is generally responsible for conducting risk management, a process through which vulnerabilities and threats to information assets are continuously assessed, and the appropriate protective controls are decided on and applied. The value of an organization lies within its infor-

## Principles of information security:

infosec programs are built around the core objectives of the **CIA triad**: maintaining the **confidentiality**, **integrity** and **availability** of IT systems and business data. These objectives ensure that sensitive information is only disclosed to authorized parties (confidentiality), prevent unauthorized modification of data (integrity) and guarantee the data can be accessed by authorized parties when requested (availability).

The first security consideration, **confidentiality**, usually requires the use of encryption and encryption keys. The second consideration, integrity, implies that when data is read back, it will be exactly the same as when it was written. (In some cases, it may be necessary to send the same data to two different locations in order to protect against data corruption at one place.) The third part of the CIA is availability. This part of the triad seeks to ensure that new data can be used in a timely manner and backup data can be restored in an acceptable recovery time.

## Threats and threat responses

Threats to sensitive and private information come in many different forms, such as **malware** and **phishing attacks**, **identity theft** and **ransomware**. To deter attackers and mitigate **vulnerabilities** at various points, multiple security controls are implemented and coordinated as part of a layered defense in depth strategy. This should minimize the impact of an attack. To be prepared for a security breach, security groups should have an incident response plan (IRP) in place. This should allow them to contain and limit the damage, remove the cause and apply updated defense controls.





## Information security vs. network security

In modern enterprise computing infrastructure, data is as likely to be in motion as it is to be at rest. This is where network security comes in. While technically a subset of cybersecurity, network security is primarily concerned with the networking infrastructure of the enterprise. It deals with issues such as securing the edge of the network; the data transport mechanisms, such as switches and routers; and those pieces of technology that provide protection for data as it moves between computing nodes. Where cybersecurity and network security differ is mostly in the application of security planning. A cybersecurity plan without a plan for network security is incomplete; however, a network security plan can typically stand alone.

## Importance of Cybersecurity

The internet allows an attacker to work from anywhere on the planet.

**Risks caused by poor security knowledge and practice:**

- Identity Theft
- Monetary Theft
- Legal Ramifications (for yourself and your organization)
- Sanctions or termination if policies are not followed

**According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:**

- Web Browser
- IM Clients
- Web Applications
- Excessive User Rights

## Cybersecurity is Safety

**Security :** We must protect our computers and data in the same way that we secure the doors to our homes.

**Safety:** We must behave in ways that protect us against risks and threats that come with technology



## Social Engineering

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

**Phone Call:**  
This is John,  
the System  
Administrator.  
What is your  
password?



**In Person:**  
What ethnicity  
are you? Your  
mother's  
maiden name?



**Email:**  
GTB Bank has  
noticed a  
problem with  
your account...

and have  
some lovely  
software  
patches!



## Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.



## Common Features of Phishing Emails

**Too Good To Be True** - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably is!

**Sense of Urgency** - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

**Hyperlinks** - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance [www.bankofarnerica.com](http://www.bankofarnerica.com) - the 'm' is actually an 'r' and an 'n', so look carefully.

**Attachments** - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.





# Online Safety Tips

Unsafe surfing can also lead to other threats—from embarrassing personal comments or images that, once online, are nearly impossible to erase, to getting mixed up with people you'd rather have had nothing to do with.

Here are the Top 10 Internet safety rules to follow to help you avoid getting into trouble online (and offline).

## 1. Keep Personal Information Professional and Limited

Potential employers or customers don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

## 2. Keep Your Privacy Settings On

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. As noted by Lifehacker, both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

## 3. Practice Safe Browsing

You wouldn't choose to walk through a dangerous neighborhood—don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you don't even give the hackers a chance.

## 4. Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. As PCWorld advises, don't download apps that look suspicious or come from a site you don't trust.

## 6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.



# BRAND AWARENESS & STORYTELLING

# LET'S START WITH WHY...



1. Understand what a brand is and how branding works
2. Understand the process and importance of developing a brand and how to measure its value
3. Identify and evaluate popular branding strategies and brand positioning
4. Be able to identify your brand and what has been lacking in it and how to move forward.

# OUR JOURNEY



## 1. Brand Concepts

*What is a Brand and Why does it Matter?*

## 2. The Distinguishing Factor

*What do all great Brands have in common?*

## 3. Good to Great

*How do you develop your Brand?*

## 4. Measuring your Brand's Value

*How do you know what your Brand is worth?*

## 5. Branding Strategies

*What will you do stand out from the competition?*

## 6. Brand Analysis

*Where is your Brand at?*



# BRAND CONCEPTS



## What is a **Brand**?

- “A product, service or concept that is publicly distinguished from others and can be distinctly communicated”
- “The experience people take away when they come in contact with you, your product, or service”
- “It is the emotional and psychological relationship you have with your customers”
- “A type of product manufactured by a particular company under a particular name”
- “The name, term, design, symbol, or any other feature that identifies one seller’s product distinct from those of other sellers”
- “It is the idea or image of a specific product or service that consumers connect with, by identifying the name, logo, slogan, or design of the company who owns the idea or image.”

# BRAND CONCEPTS



What is a **Brand**?

A **brand** is the **personality** of a business.

– Alan Dibbs

# BRAND CONCEPTS



## **Your Brand Components:**

- Name
- Design
- Communication
- Promise (value proposition)
- Target Market
- Awareness

# BRAND CONCEPTS



## Other Key Concepts

- Brand Awareness/Visibility: The **reach** of your Brand or extent to which your Brand is well known, by those who matter.
- Brand Equity: The **goodwill** you build up that compels people to choose you over the competitor.
- Brand Storytelling: The **message** you communicate that propels your audience to action.



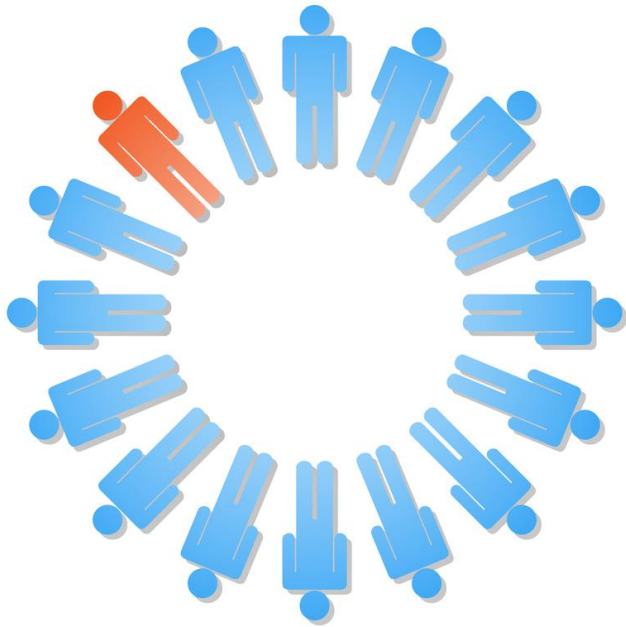
# THE DISTINGUISHING FACTOR

What do all great Brands have in common?



# THE DISTINGUISHING FACTOR

What do all great Brands have in common?



1. They know their Audience
2. They have a Clear Promise
3. They are Unique
4. They are Consistent
5. They use great Storytelling
6. They Engage their customers
7. They are Authentic

# FROM GOOD TO GREAT

How do you go from just being a logo & a name to being a Brand?



## Tell a good Story

People don't care about your product, they care about themselves."

1. Define your Target – problem, picture, niche
2. Use relatable Data – gain authenticity by backing emotions with figures
3. Use persuasion effectively – engagements and reviews

# BRAND ANALYSIS

Let's get practical about your Brand





THANK YOU



# SOCIAL MEDIA & MASTERING THE ART OF DIGITAL STORYTELLING

If you want to get consumers' attention, try **telling a story**. If you want to reach them where they're already engaged, tell your story online.

As digital storytellers, brands can utilize technology and computer-based tools to share their messages. This practice spans endless digital storytelling tools and narratives, including text, images, video, audio, social media, website, mobile app and interactive elements.

With the right narrative, brands can speak to their consumers in a way that resonates. Stories create a conversation with the audience, rather than brands simply talking at their customers.

Not only do people understand stories, they also like them. Telling a story allows brands to successfully present concepts to their audience and form a connection that goes beyond products or services.

Think about Coca-Cola. The brand's story is more than selling a refreshing drink. **Instead, opening a bottle of Coke is a way to share happiness and love.** The iconic 1971 "I'd Like to Buy the World a Coke" spot originally got the world's attention by creating a caring, welcoming and united community of Coke drinkers.

Tell a story that appeals to emotion and feels relatable to your consumer.

## Social Media & High Engagements

*Pishon... "impossible doesn't exist"*

[www.pishondesigns.org](http://www.pishondesigns.org) | +2348086816356 | [issues@pishondesigns.org](mailto:issues@pishondesigns.org)

Social media engagement is an important metric to consider when building an online store. While most want to increase the size of their audience, they often fail to increase their social media engagement as well. When you engage with your followers on social media you can turn them from fans into customers.

The time you devote to building relationships with your audience can lead to a higher number of sales, increase in customer loyalty, and higher positive reviews.

The most common and expensive way to grow your followers is to spend money on **advertising**. You can also buy ads to increase your followers on Facebook, Instagram, or Twitter. While you will grow your followers, they might not have the same level of commitment as someone who discovered your brand through an amazing product ad.

If you're just starting out, you'll also want to **create unique content**. (See storytelling tips). You'll want to have a mix of your own content and popular content you've found on the internet. If sharing someone else's content always credit them on your page. When it comes to your own content, you can create quote graphics, funny gifs, viral videos, and more. Creating your content can take time to create. However, with long term effort, you'll find that you eventually get more shares which will help you to grow your social media following.

You can also grow your followers by **engaging with your customers**. Being active on your social media pages will show that your page is worth following. By posting content regularly, communicating with your customers, people will naturally follow your page. You'll also grow followers when you engage with customers who don't necessarily follow you. They'll be more likely to follow your page when you build relationships with them.

*Pishon... "impossible doesn't exist"*

[www.pishondesigns.org](http://www.pishondesigns.org) | +2348086816356 | [issues@pishondesigns.org](mailto:issues@pishondesigns.org)

Having a **consistent theme** on your social media accounts can also increase your followers. A theme can be the type of content you share (funny, inspirational) or the look of your content (minimalist, colorful). How do you want your brand to be perceived by others? Focus on creating a consistent personality and voice for your content.

**Collaborations** with other brands can also help grow your followers.

You'll want to collaborate with other brands who have a similar audience but sell different types of products. -----For example, if you sell jewelry you could collaborate with another brand that sells accessories like scarves. You'll be able to tap into each other's audiences to grow your followers. A collaboration might include a contest, giveaway, blog post promoting their products, or post on social media.

## **Tools to download:**

- CANVA
- BUFFER
- IFTTT
- HOOTSUITE

They help in scheduling.

## Other notes

- Look at examples of brands that have blown up and their strategies no matter your field.
- How will you apply this knowledge?
- What are your next steps?

*Pishon... "impossible doesn't exist"*

[www.pishondesigns.org](http://www.pishondesigns.org) | +2348086816356 | [issues@pishondesigns.org](mailto:issues@pishondesigns.org)