The Value of Information

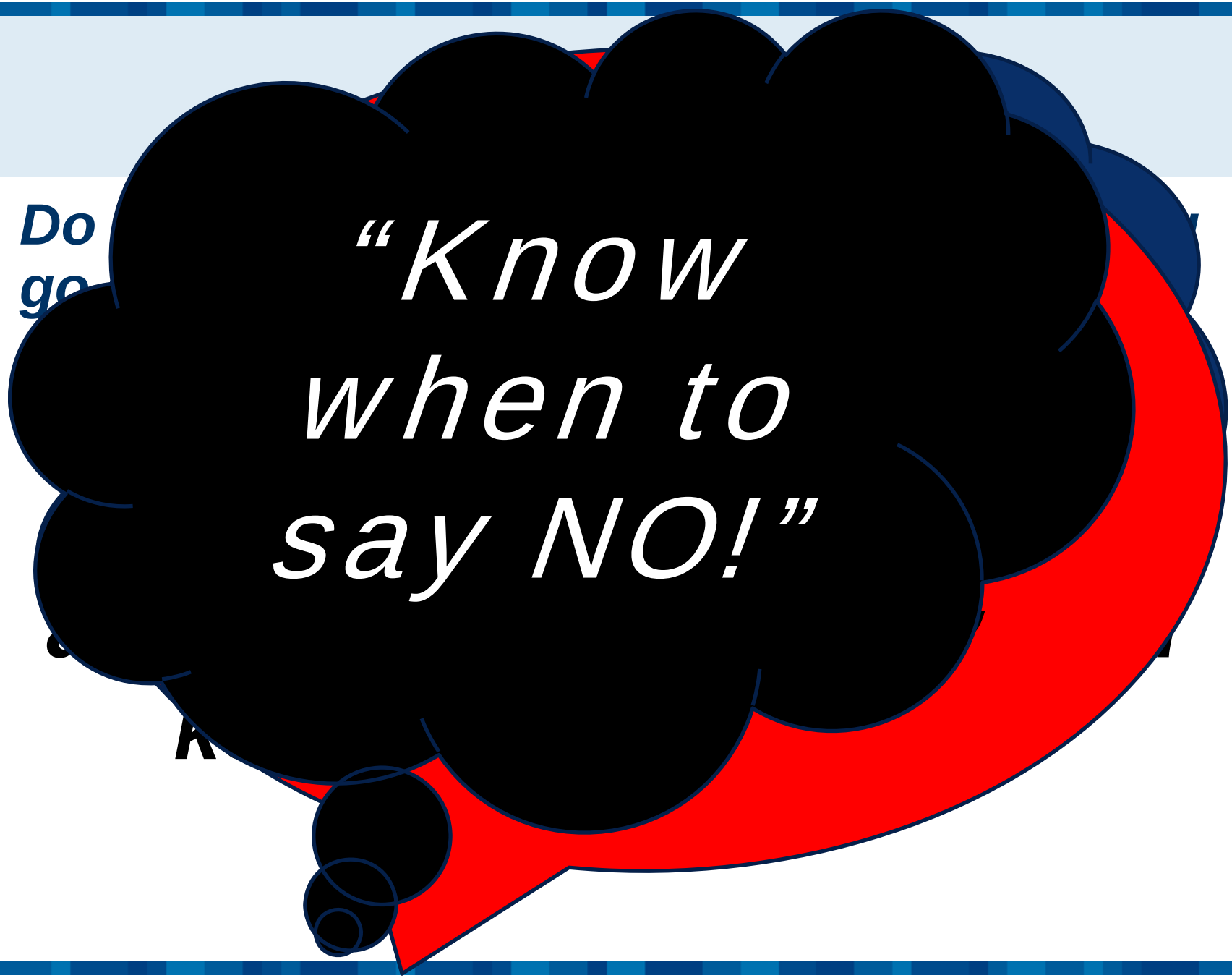
What's Their Motivation??

So, who is the target???

How Trusting Are You?

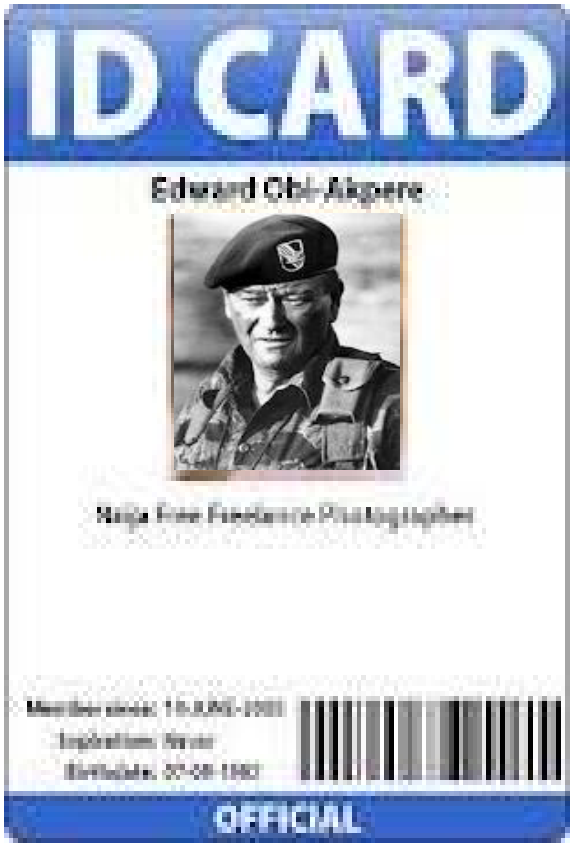
Trust but Verify!!

The Issue



Okay, let's take a breath!

Games



Convenience vs. Security

Interesting Comments I have Heard

- **“I’m not worried about it”**
- **“My computer company said I am secure”**
- **“I don’t have anything the hackers want”**
- **“I have a really good password. It’s really long!!!!”**
- **“That is not my area, IT is responsible for securing info!!!!”**
- **“Its not my information, and its not my job.”**

The Risk

- What's the Risk of bad security practices?
  - National security issue?
  - Embarrassment?
  - Loss of Revenue?
  - Bankruptcy?
  - Loss of customer confidence?
  - Loss of proprietary data/trade secrets?

The Liability

- **Who's liable when information is lost or stolen?**

YOU!!

- **One of consumers' biggest fears is identity theft!**
- **Loss leads to fines, lawsuits, and negative reputation!**

Must Have Security

- **Compliance, depending on your industry requires security.**
- **Commonsense and your fiduciary responsibility requires good security.**
- **As an employee, you have a responsibility to protect company information.**

How To Reduce Risk – Eliminate Liability

1. Determine what information you are collecting, processing, and storing
2. Who has access to that information
3. Categorize the info based on sensitivity
4. Write the policies showing how info is secured, protected; and to educate employees on their responsibilities
5. Train, train, train

Policy Must Haves

- Policies outline how the company is implementing security – so, a security policy is a MUST
- Policies provide employees notice of do's and don'ts, as well as their responsibility
- Some other policies: social media, BYOD, wireless, work from home, password, Internet usage or AUP, etc. Also, for certain industries, compliance policies.

What did we learn?

- ***Hackers/thieves want everything, not just credit card #'s.***
- ***Mobile devices have increased the threat!***
- ***Stealing data/info is relatively easy!***
- ***It can lead to catastrophic consequences.***
- ***Training is the key.***
- ***Keep training interesting, fun, and interactive.***
- ***Take a personal interest in protecting all info, not just your own!***

Cybersecurity Tips!

- ***Don't bank on your smartphone***
- ***If banking online, make sure the bank window is the only one open, and the URL says Https***
- ***When using public WiFi, like a coffee shop, airport, hotel, use a proxy like Hotspot***
- ***Don't click on links in email, go to the site like Facebook, LinkedIn, etc.***
- ***When you can, encrypt all data***
- ***Don't click on the "unsubscribe" link on unwanted emails. It validates your email and may add you to spam.***

BLUF

- End User is the Target

- Train the Workforce to:
  A. Recognize the threat
  B. Recognize the scams
  C. Understand the Value of Information

- Training should be:
  A. Interesting
  B. Engaging
  C. Continuous

Don’t Be This Guy!!

commended Global Knowledge Courses

Certified Ethical Hacker v7

Cybersecurity Foundations

Foundstone Ultimate Hacking

Defending Windows Networks

Cybersecurity Mobility & Compliance Course (CSMCC)

www.globalknowledge.com
1-877-333-8326

Global Knowledge®