Hackers are After You!
Protecting Yourself from the Evils of the Internet

Steve McEvoy
October 20th, 2023

A note about my online version:

I strip the graphics out of my online version of presentations just to remove any possible copyright infringement.

Boring I know, but the discussion is what matters.
Thanks for attending! Steve

Fun!

Entertaining!

The Internet is _____

Unruly

Scary

Dangerous

(Cyber) Security is _____

Annoying

Confusing

Complicated

Difficult

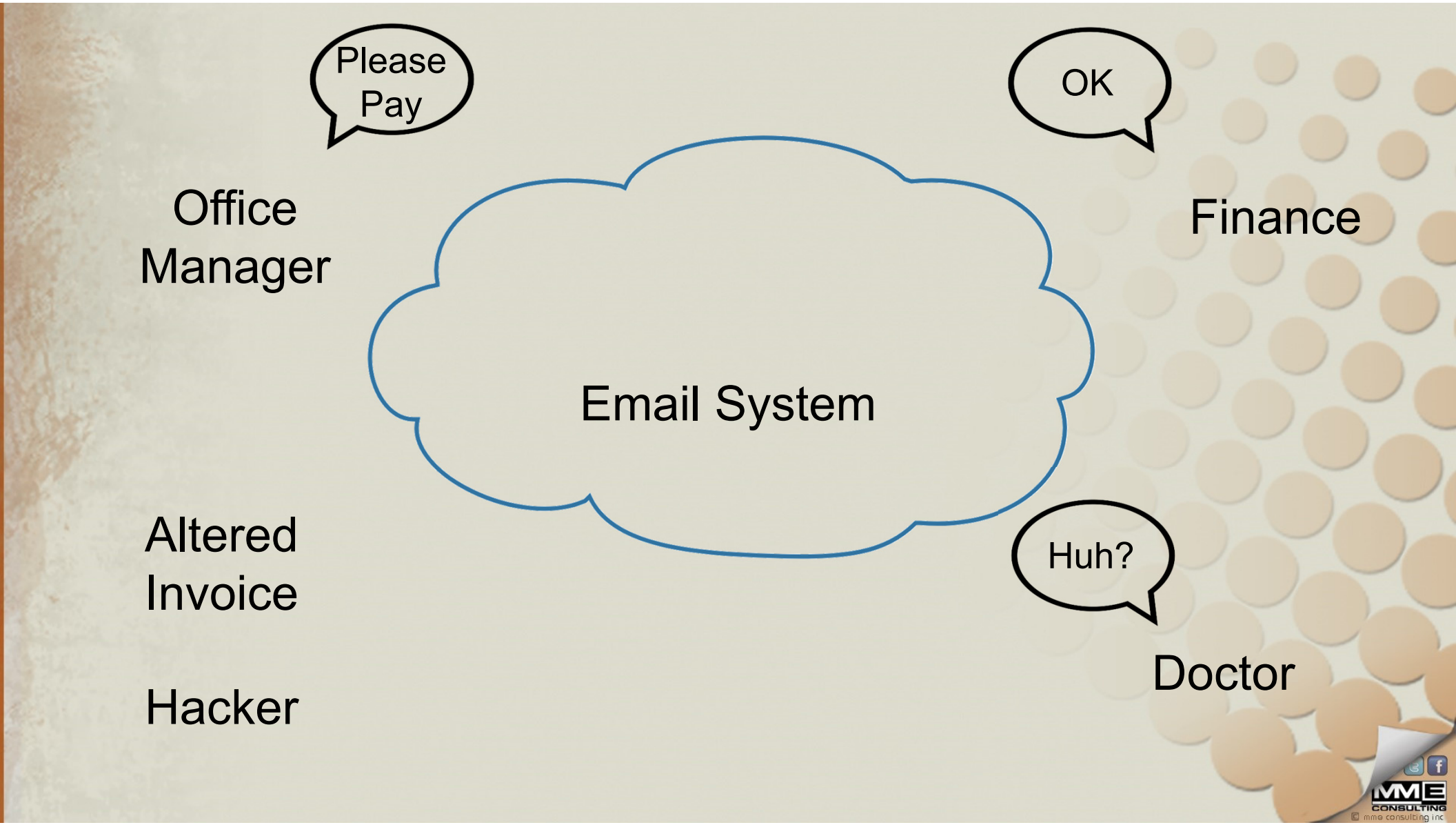
Expensive

How can you be 100% safe from Cyber crime with little effort?

The Internet has some scary s**t going on

This is a self defense course

Let me tell you a story …

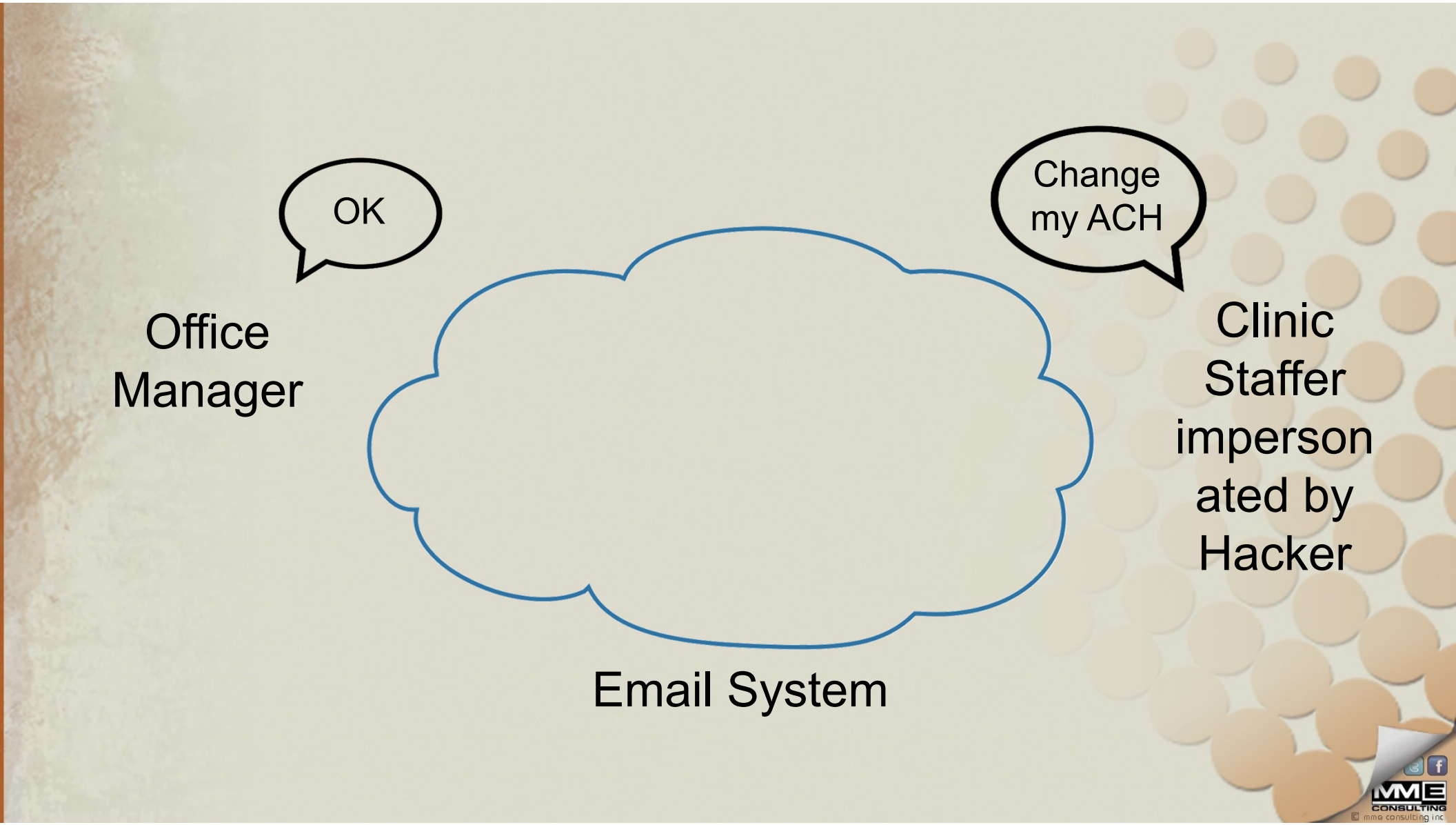

Please Pay
OK
Office Manager
Finance
Email System
Altered Invoice
Huh?
Doctor
Hacker

Technology Fails

- Manager Reused Password
- MFA Not Enabled for email accounts
- Manager was an email 'Admin' unnecessarily
- Geo-Blocking not enabled
  - (Hacker was in Sweden)

Size of the Haul?

About $1,000


OK
Change my ACH
Office Manager
Clinic Staffer imperson ated by Hacker
Email System

Technology Fails

- Clinic User Reused Password
- MFA Not Enabled for email accounts

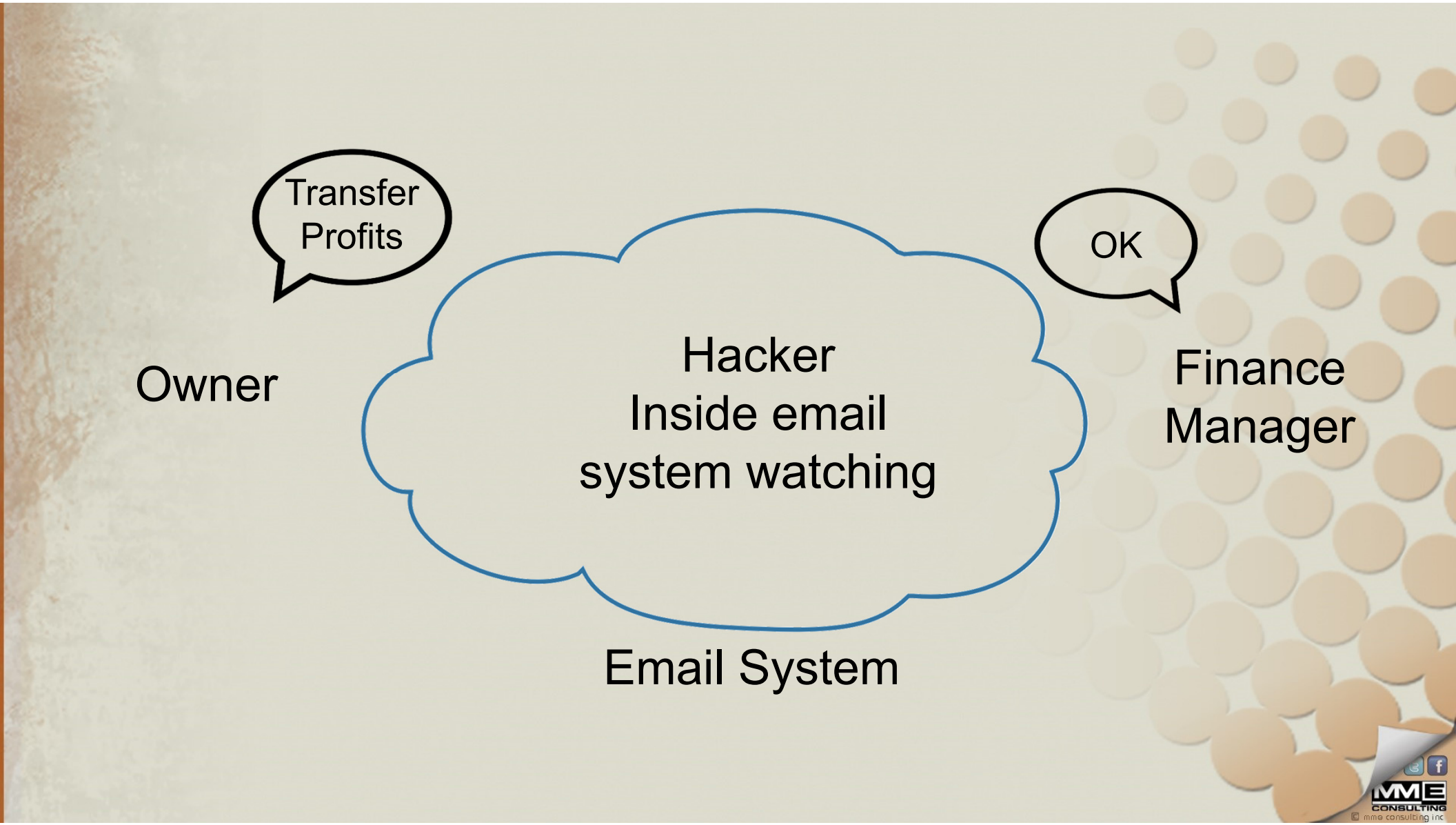
Size of the Haul?

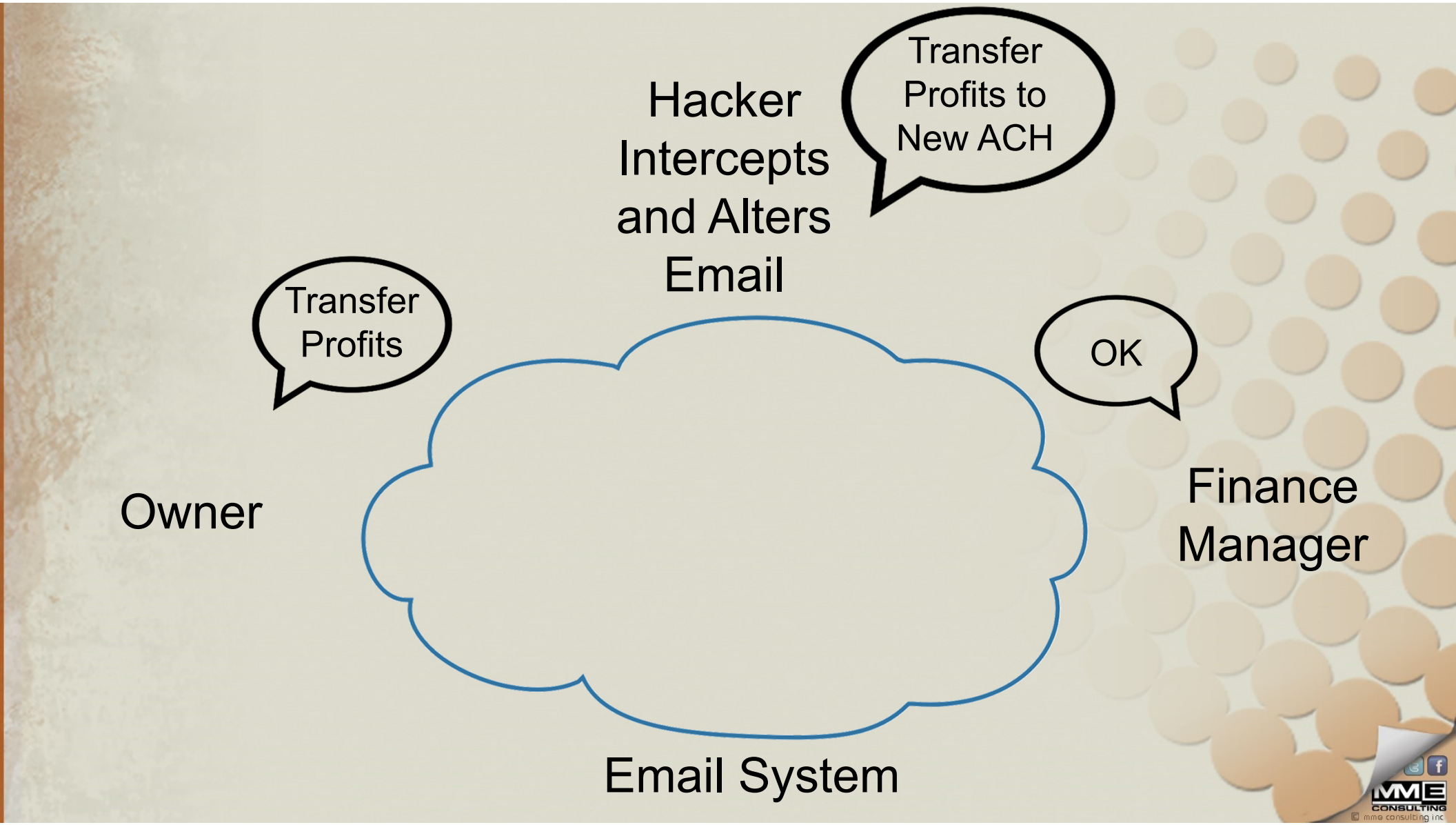
About $5,000

Just one more …

Size of the Haul?

>$500K


Transfer Profits
OK
Owner
Hacker
Inside email
system watching
Finance
Manager
Email System


Transfer Profits to New ACH
Hacker Intercepts and Alters Email
Transfer Profits
OK
Owner
Finance Manager
Email System

Solution for All Three Events?

- No Technology Required!
- Free!
- Almost no Training Required
- Can be implemented TODAY!

Solution for All Three Events

An Actual
Phone Call

Financial Change Policy

- Any change in a payment process needs verbal confirmation with the requestor
  - New vendor
  - New account
  - Change of money flow of any kind
- Independent confirmation by the person processing
  - You call them to verify

Security's Weakest Link?

Our Staff

“Social Engineering”

A term used for a broad range of malicious activities **accomplished through human interactions**.

It uses psychological manipulation **to trick users** into making **security mistakes** or giving away sensitive information.

"Social Engineering"

Attacks happen in **one or more steps**.

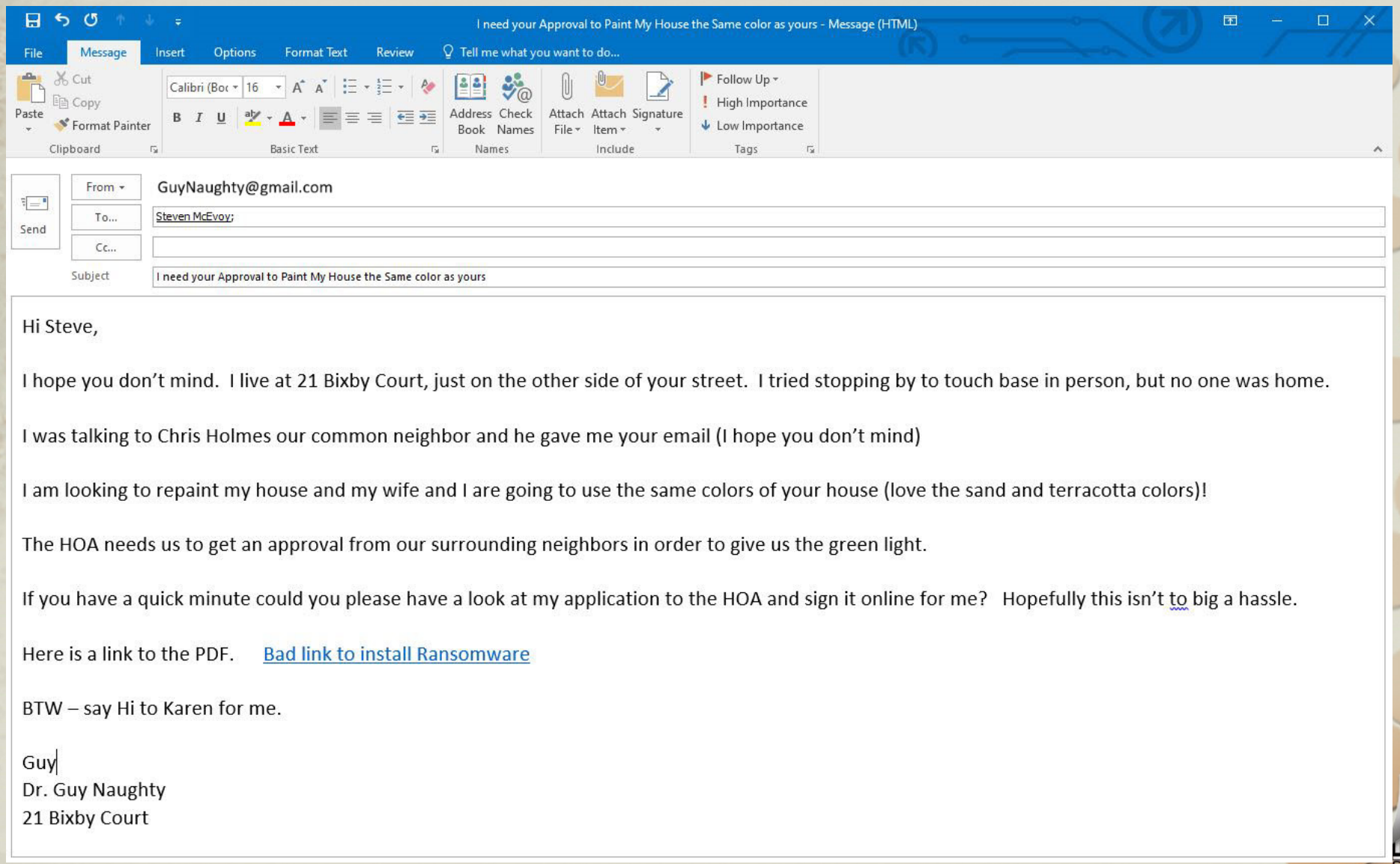
A perpetrator first **investigates the victim** to gather background information needed to proceed with the attack.

Then, the attacker moves to **gain the victim's trust** and **tricks them** into revealing sensitive information or granting access to critical resources.

Spear Phishing

What we can learn from a single picture…

- White
- Male
- 50’s ish
- Probably Married
- Not Broke
- Exactly where I live
- What my house looks like
- Who my neighbors are


I need your Approval to Paint My House the Same color as yours - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Tell me what you want to do...
Cut
Copy
Format Painter
Paste
Clipboard
Calibri (Bo
16
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Follow Up
High Importance
Low Importance
Tags
Send
From
GuyNaughty@gmail.com
To...
Steven McEvoy;
Cc...
Subject
I need your Approval to Paint My House the Same color as yours
Hi Steve,
I hope you don't mind. I live at 21 Bixby Court, just on the other side of your street. I tried stopping by to touch base in person, but no one was home.
I was talking to Chris Holmes our common neighbor and he gave me your email (I hope you don't mind)
I am looking to repaint my house and my wife and I are going to use the same colors of your house (love the sand and terracotta colors)!
The HOA needs us to get an approval from our surrounding neighbors in order to give us the green light.
If you have a quick minute could you please have a look at my application to the HOA and sign it online for me? Hopefully this isn't to big a hassle.
Here is a link to the PDF.
Bad link to install Ransomware
BTW – say Hi to Karen for me.
Guy
Dr. Guy Naughty
21 Bixby Court

Meet Dr. Thomas & Team

Me the Hacker **VS.** Dr. Thomas's Office

What can we learn online about Dr. Thomas's office?

What can we learn online?

- Practice Name
- Doctors Name
- Where its located (and time zone)
- Orthodontic Practice
- Windows Computers (?)
- X-ray machine (?)

What do we know so far?

- ThomasOrthodontics.com
- Thomas Orthodontic
- Dr. Larry Thomas
- California Office
- Orthodontic Practice
- Windows Computers
- CBCT X-ray machine
  - But I don’t know what model (yet)

And with a bit more research …

- Who sells that brand of X-ray Machine (?)
- Where that Company is located
- What's the Average Fee for Orthodontic Services

How would you Phish them?

- Email?
  - Unsolicited Resume with infected PDF attached?
  - Some sort of scam for the X-ray machine?
- How about a Phone Call?

To learn what brand of X-ray

https://youtu.be/k7V0KQgSgJo

And with a bit more research …

- Dexis Imaging makes the iCAT
- Dexis support of iCAT is in Philadelphia

DEXIS™

And now for the win …

A couple of weeks later I place another call

https://youtu.be/545W1OY2aoY

With about 15 minutes of time invested …

- Got a staff member to click on a link
- Accessed Patient Information
- Copied software to a computer in the office and ran an application
- Gathered information about their network
- Copied information out of their office
- Gathered more social engineering info for a future hack if needed

What could they have done?

- Question the validity
- Ask Dr. Thomas if he asked for this
- Call them back
- Never let a stranger onto you computer or device (ever!)
- Make it David's the IT guys problem

What Should You Do?

Take Aways…..

- Ensure your IT Person has secured your email system:
  - Require hard and unique passwords
  - Require MFA for ALL accounts
  - Reviewed who is an admin
  - Enable Geo-Blocking to stop access outside USA

Take Aways…..

- Establish a Financial Change Policy
  - Any request has to be verbally verified with the expected requestor
  - Write the policy down
  - Explain this presentation to your team
  - Cyber Insurance is starting to require this policy

Take Aways…..

- Be Wary – understand Social Engineering
  - Question requests for access
  - Call them back using published numbers
  - When in doubt – punt! Take the time to be sure.

Who has done 23andMe?

- Was hacked in recent days for information
  - Used usernames/passwords from other data leaks
  - Skimmed shared information of genetic relatives
- Login and:
  - Change your password
  - Enable MFA

Thank You!

Presentation online at
www.mmeconsulting.com/Presentations

steve@mmeconsulting.com

MME CONSULTING
MMEconsulting.com

Technology Planning and Integration for Dental Specialists