

# Security Awareness for Executive Management

How to Gain Buy-In

Kathryn Merhout  
Regional Information Security Officer, DBHDS

# Why?

- Security must be non-negotiable
- Executive buy-in
- ISO and Executive partnership



# Target Audience

- Who is the security training for?
  - Identify role and objective of training required for specific roles
    - Agency Head
    - Middle Managers
    - Executive Assistants

# Super Secret Decoder Ring Instructions

- Leverage your Executives ability to “encourage”
  - Policy Acceptance
  - Clarify Employee Responsibilities
  - Influence Change



# Conversations With Executives

- Opens up to discussions of:
  - Risks at the Agency
  - Resources Needed



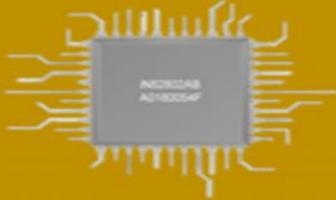
# Job Security

- More Status Reports
- Metrics
- Responding to more questions



# Heart Heart

- Build Trust with Executive Team
- Knowledge Share
- Geek Speak
- Business Drivers
- Realistic Expectations
- Emphasize Executive Level Involvement

Word of the Day	Layman Speak	Geek Speak
<b>Chips</b>		
		

# Change in the Exchange

- Enterprise Level
- Expected & Respected Topic
- Business Requirement
- Provide Benchmarking

# Executive Security Awareness

## Why IT Matters



# Why are you here?

- ***Vital role*** in being a line of defense against hackers
- ***Be aware*** of the growing Cyber Security threats Executives face
- ***Be sensitive*** to what is happening around you



# TOP 3 CYBER THREATS

facing organizations in 2016:



SOURCE:

ISACA'S JANUARY 2016 CYBERSECURITY SNAPSHOT, GLOBAL DATA,

[WWW.ISACA.ORG/2016-CYBERSECURITY-SNAPSHOT](http://WWW.ISACA.ORG/2016-CYBERSECURITY-SNAPSHOT)





# Social Media *Got'cha!*

- [Jack Vale Films on You Tube](#)

# Spear / Whale- Phishing Awareness



Hackers target Executives for multiple reasons, and may have multiple agendas.

- Personal - revenge for being fired or some belief that the company wronged them.
- Political - The company has wronged others or they are part of an activist group targeting companies or individuals for their actions.
- Financial - Monetary Reward: steal funds, or intellectual capital to sell on the dark web's black market.
- State Sponsored- Groups financial funded by governments to target companies for corporate espionage to gain market place advantage.

# Most Common Security Mistakes



- Poor password management
- Leaving your computer on, unattended
- Opening email attachments from strangers
- Sharing information (passwords and machines)
- Not reporting security violation

**Decisions we make are essential to protecting information and systems.**

# Security Threats To Be Aware Of

- **Social Engineering**
- **Phishing Scams**
- **Viruses, Spyware and Worms**
- **Shoulder Surfing**
- **Dumpster Diving**



# Social Engineering

Social engineering manipulates people into performing actions or divulging confidential information. It is the clever manipulation of the natural human tendency to trust.

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

**Email:**  
ABC Bank has  
noticed a  
problem with  
your account

I have come  
to repair  
your  
machine...



and have  
some  
software  
patches



# Securing Against Social Engineering



Impersonation may occur over the phone, in person or via e-mail.



Tailgating - be cautious of individuals following you through secure doors.

**Be aware of your surroundings!**

# Be Aware of Social Engineering Attacks



- Thief acting like an employee
- Using social skills to penetrate network
- They ask a lot of questions to collect information
- May offer credentials to support stolen identity

Report suspicious activity to **(enter your information)**

# Don't Get Tricked by False Advertisement!

- Ads can come from social media websites, via email, websites or instant messaging
- Opening an attachment or clicking of a link could trigger a virus download.
- **If you don't know what it is or where it came from, don't open or click on it!**



# Did you know? At Virginia COV Agencies

Spam accounted for **730** million messages at Commonwealth last year

These messages were automatically identified and blocked as SPAM, phishing or malicious emails.



# Don't Get Hooked by Phishy Scare Tactics!



## WINDOWS SECURITY CENTER ALERT!



### Windows has detected an Internet attack attempt...

Somebody's trying to infect your PC with spyware or harmful viruses. Run full system scan now to protect your PC from Internet attacks, hijacking attempts and spyware!

Click here to download spyware remove for total protection.

Scareware scammers use fake versions of virus alerts and other system problem messages.

Pressing **ALT-F4** immediately on your keyboard will shut down your browser and stop any scareware from getting downloaded.

# Phishing Email Examples

**Enter an example of a phishing email from your company. Enter as many examples that will resonate with your audience.**

# Phishing Email – Where do links take you to?

Subject: Your Bank of America accounts has been locked! Date: 3/4/2013 7:29:17 P.M. Pacific Standard Time From: [onlinebanking@alert.bankofamerica.doc.com](mailto:onlinebanking@alert.bankofamerica.doc.com)

Exclusively for: | VALUED CUSTOMER

Online Banking Grammar errors

Bank of America



**Your Bank of America accounts has been locked!**

## Unprofessionally written

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please [click here](#) to continue the verification process and ensure your account security.

<http://solucionesintegraleseninternet.com/jennyfer/store//login/>



Phishing link: Hovering over the link reveals a foreign and suspicious link

# Tips for Securing Your Work Area



- **Lock** your screen when you step out of your work area
- **Do not** leave mobile devices or thumb drives lying around
- **Lock** file cabinets, overhead bins, and desk drawers when unattended and make sure the keys are secure
- **Ensure** sensitive documents are stored away

**Remember, information security is everyone's responsibility!**

# Choose a Secure Password!



- Easy to remember
- Don't write it down
- The longer the better
- Mix of random letters, numbers and special characters, etc.
- Password resets must be called into the Help Desk by the person who owns the account

**Never share your user id or password with anyone.**

# Password Cracking: Dictionary Attack and Brute Force

Pattern	Calculation	Result	Time to Guess ( $2.6 \times 10^{18}$ /month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	$26^4$	$5 \times 10^5$	
8 chars: lower case alpha	$26^8$	$2 \times 10^{11}$	
8 chars: alpha	$52^8$	$5 \times 10^{13}$	
8 chars: alphanumeric	$62^8$	$2 \times 10^{14}$	3.4 min.
8 chars alphanumeric +10	$72^8$	$7 \times 10^{14}$	12 min.
8 chars: all keyboard	$95^8$	$7 \times 10^{15}$	2 hours
12 chars: alphanumeric	$62^{12}$	$3 \times 10^{21}$	96 years
12 chars: alphanumeric + 10	$72^{12}$	$2 \times 10^{22}$	500 years
12 chars: all keyboard	$95^{12}$	$5 \times 10^{23}$	
16 chars: alphanumeric	$62^{16}$	$5 \times 10^{28}$	

# If you see something, say something!



- Suspicious activity on computer system
- Theft/loss of information storage device
- All phishing emails
- Unauthorized access to restricted information

Report suspicious activity To **(enter your information)**

# Questions?



# Discussion

- Need Metrics? Contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)
- You Tube Video: *Jack Vale Films*
- Another Resource: <http://www.silverbull.co/cybersecurity-awareness-for-business-executives/>
- Another example of SA for Executives: <http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/infosecurity-executives.pdf>
- Copy of this presentation? Email [Kathryn.Merhout@DBHDS.Virginia.Gov](mailto:Kathryn.Merhout@DBHDS.Virginia.Gov)