Erich Kron
Security Awareness Advocate

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)²
- A veteran of IT and Security since the mid-1990’s in manufacturing, healthcare and DoD environments
About Us

• The world's most popular integrated Security Awareness Training and Simulated Phishing platform

• Based in Tampa Bay, Florida, founded in 2010

• CEO & employees are ex-antivirus, IT Security pros

• Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer

• 200% growth year over year

• We help thousands of organizations manage the problem of social engineering
“All warfare is based on deception.”
- Sun Tzu, *The Art of War*
98% of Attacks Rely on Social Engineering

Attackers go for the low-hanging fruit:

humans
Agenda

• The Perception vs. Reality dilemma
• Understanding the OODA (Observe, Orient, Decide, Act) Loop
• How social engineers and scam artists achieve their goals by subverting its different components
• How we can defend ourselves and our organizations
The Perception vs. Reality dilemma
Understanding the OODA (Observe, Orient, Decide, Act) Loop
How social engineers and scam artists achieve their goals by subverting its different components
How we can defend ourselves and our organizations
Pick a card!
Is it gone now?
How did we identify and remove your card?

Here’s what we started with:

And here’s what we ended with:

Yeah: These are two *completely different* sets of cards. But, by *rushing* you through the process, you probably didn’t notice!
Our brains’ job to filter, interpret, and present ‘reality’
What is REALITY?

Yanny
-or-
Laurel?
Agenda

- The Perception vs. Reality dilemma
- Understanding the OODA (Observe, Orient, Decide, Act) Loop
- How social engineers and scam artists achieve their goals by subverting its different components
- How we can defend ourselves and our organizations
An Interesting History

Using our brain’s strengths against us

Left hand lowered for action immediately after match is struck.

http://ciamagic.com/
An Interesting History

Using our brain’s strengths against us

Left: Normal expression of face. Right: Exaggerated expression of
dumbness. The more facial muscles are relaxed and eyes thrown out
of focus, the greater the effect. Doing these actions to a mild degree
merely shows a lack of alertness or disinterest.

http://ciamagic.com/
Spies, Magicians, Pickpockets, Con-artists and Cybercriminals all use the principles we are about to discuss
OODA

A Model for Decision Making
What is an OODA Loop and how do I mess with it?

“In order to win, we should operate at a faster tempo or rhythm than our adversaries—or, better yet, get inside [the] adversary's Observation-Orientation-Decision-Action time cycle or loop ... Such activity will make us appear ambiguous (unpredictable) thereby generate confusion and disorder among our adversaries—since our adversaries will be unable to generate mental images or pictures that agree with the menacing, as well as faster transient rhythm or patterns, they are competing against.”

-- John Boyd (creator of the OODA Loop)
Agenda

- The Perception vs. Reality dilemma
- Understanding the OODA (Observe, Orient, Decide, Act) Loop
- How social engineers and scam artists achieve their goals by subverting its different components
- How we can defend ourselves and our organizations
“I’ve never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads.”

Elliot Alderson
The ideal situation for a social engineer is to hijack the OODA loop by creating a knee-jerk action that effectively bypasses the first three steps and results in the attacker’s intended Action.
Attackers will do anything to bypass critical thinking

- Spoofs a campus-wide security alert for a community college (confidential information blocked out) in Florida.
- Exploits current concerns over active shooters on education campuses
- Crafted to generate a reflexive click.
- Directs to credential capture site.
- Other variants seen:
  - “IT DESK: Security Alert Reported on Campus”
  - “IT DESK: Campus Emergency Scare”
  - “IT DESK: Security Concern on Campus Earlier”
Example: Business Email Compromise (The Phish Evolved)

- a.k.a. CEO Fraud
- No payload
- Low volume email targeting high value individuals
- Personalized
- Few to no ‘traditional’ spam/phishing tells (such as poor grammar, egregious misspellings, etc.)
Example: W2-Fraud

**Urgent Request**

**Stu Sjouwerman**<slus@knowbe4.

7:50 AM (1 hour ago)  

to me

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

---

**Re: Urgent Request**

Hi Alanna,

Thanks for your quick response. I will want you to kindly work with Kim and get the list of W-2 copy of employees wages and tax statement for 2015. Make sure they are in PDF file type and send it as an attachment. Kindly prepare the lists and email them to me asap.

Thanks,
Stu
Example: The Invoice/P.O. Phish

- The most common phishing genre in the emails reported to us via the Phish Alert Button (PAB)

- This type of phish easily blends into the deluge of emails that employees in many positions deal with on a daily basis.
Companies and organizations in the business of delivering packages and parcels now email customers and users on a daily basis.

Once again, the bad guys regularly seek to capitalize and exploit this kind of business-to-business communication by crafting phishing emails that mimic those sent by recognized organizations like USPS, UPS, FedEx, and DHL.
Example: Gift Card Scams

From: executive@pharmsa.com
Message-ID: <1758473657.82816.1549554140411@webmail.pharmsa.com>

----
Hi Liz,

I need you to make a purchase of Itune Giftcard this morning. It's a gift for a vendor, Are you available to make the purchase now?

Best Regards,
Patrick. (edited)
Example: Payroll Redirection

Subject: Eft dd info update
from=pavinski1810991ua@gmail.com
To: (Payroll)
(Payroll),
I 'll like to change my EFT dd info, can it be effective for the current pay date ? My old account is closed and i changed to a new financial institution.

Regards
(CEO) (edited)
Example: Tech Support Scam

** Microsoft Warning Alert **

ERROR # 268d3x8938(3)

Please call us immediately at:
+1-(888)-919-6150 (Toll Free)
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.
Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware. The following information is being stolen...

1. Facebook Logins
2. Credit Card Details
3. Email Account Logins
4. Photos stored on this computer

You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity or from any information loss.

Call Microsoft: +1-(888)-919-6150 (Toll Free)
Clickbait: It’s More Science Than You Think

• Leverages “pattern interruption” to create curiosity often based on the "information-gap" theory

• “Such information gaps produce the feeling of deprivation labeled curiosity. The curious individual is motivated to obtain the missing information to reduce or eliminate the feeling of deprivation.” - George Loewenstein, Carnegie Mellon

• Also leverages outrage and anger, which drives us to take action
Agenda

• The Perception vs. Reality dilemma
• Understanding the OODA (Observe, Orient, Decide, Act) Loop
• How social engineers and scam artists achieve their goals by subverting its different components
• How we can defend ourselves and our organizations
COMMON "IN THE WILD" ATTACKS

- Wells Fargo: You have a new secure mail
- Undelivered Mail
- Etrade: Action Required!
- Microsoft Teams: Rick sent a message
- Microsoft/Office 365: Action required: Update your payment information now
- Stripe: Just now someone logged in to your account
- HR: Your Action Required
- Amazon: Refund Notification
- OneDrive: Your OneDrive is out of storage space
- HR: Download your W2 now

KEY TAKEAWAY

The common theme we see here is the push for action required. One message even has an exclamation point, which emphasizes the urgency of the message. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.
Are You Being Manipulated?
-- understand the lures --

Greed  Curiosity  Self Interest
Urgency  Fear  Helpfulness
Where are you **distracted?**
Social Engineering Red Flags

FROM
- I don't recognize the sender's email address as someone I ordinarily communicate with.
- The email is from someone outside my organization and it's not related to my job responsibilities.
- The email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like microsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

DATE
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

SUBJECT
- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

TO
- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

CONTENT
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click on a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?
New School Security Awareness Training Programs Work

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type and organization size**
- **241,762** Phishing Security Tests (PSTs)
Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com | @KB4Erich | @ErichKron