
the upside of risk
LanierUpshaw
Assurex
GLOBAL
Cyber Security and the Human Factor

The Hacker

News after news story for the past few years has made us all leary of this guy. . . The hacker. He is a threat to our personal and business information. He targets sensitive information about our clients, partners, intellectual property and employees. They threaten our business reputation and can do damage that is unquantifiable by over taking our public voice in social media.

The Hacker's Trophies: 2017 Ed.

Feb: InterContinental Hotels Group (IHG) responsible for popular hotels such as Crown Plaza, Holiday Inn, Candlewood Suites and Kimpton Hotels announced malware based breech that affected 12 properties. Credit Card holder names, card numbers, expiration dates and internal verification codes were obtained. After further investigation they found later in the year that there was a much larger scope of locations affected.

Feb: Arby's – Malware based credit card pilfering. About 1,000 corporate restaurants affected. Scope/size/reach of breach – not completely known.

March: River City Media. A group of spammers. The hackers had the bad guys! Well, not quite. RCM didn't realized they had released their private data into the websphere when they didn't configure their backups properly. This one became known as Spammergate. Good guys found the information first – but databased was worth 1.4 billion email accounts, IP addresses, full names and some physical addresses.

What are they looking for?

- Credit Card Information through point of sale systems
  - Hotels, restaurant chains, retail
- Personal Identifiable information
  - Student, customer, user databases

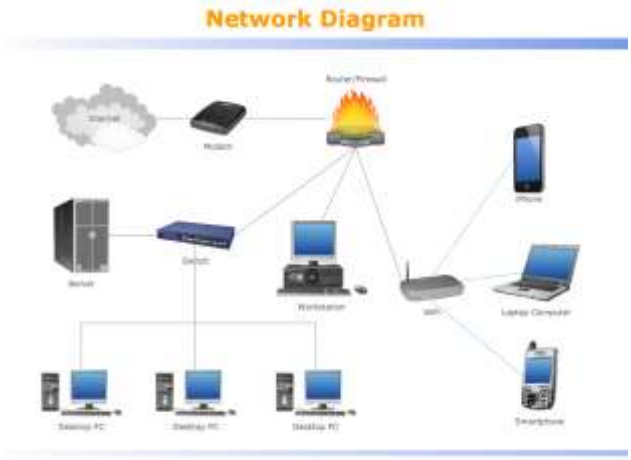
Dollar Bills!!

- 2016 Data from Avast Security claims:
  - Credit cards without a balance: $8 per card (number and CVV)
  - $2000 balance guarantee: $20 per card (number and CVV)
  - Driver's license scans: $20
  - Email Addresses and passwords: $0.70-$2.30
  - Social Security Numbers: $1 ($1,25 for state selection)
  - Paypal credentials/access: $1:50

There is a market for these things they are collecting. The Hacking economy is so advanced that if you take the time and verify that your data is valid, you can fetch a higher price for the information you are selling. So you have the pirate, the information processor who will help you validate the information, a broker to play middle man between the buyer and the seller. And their market suffers the same supply and demand forces we deal with daily.

So, we know that this economy is largely focused on obtaining Personal Identifiable information – or commonly referred to as PII.

Surveying the Landscape



Our original security assessments ‘back in the day’ were typically from the ‘physical’ standpoint. Have a firewall. Put a password on your desktop. The endpoints were the focus of security strategies. Best practices have not gone away for this and continue to become more sophisticated. Most people still think about that Hacker sitting in Starbucks with a French press or at home with a bag of twizzlers and a coke poking away trying to find the mouse hole in.

Introducing The Human Factor

But then our little friend got smart. And he said you know what, I bet you someone will make this easy for me. And humans became their targets. Humans are the wild card and they do their best to capitalize on this.

And the label ‘Social Engineering’ is born

The basic concept is, manipulate the poor people and they will open the door for you

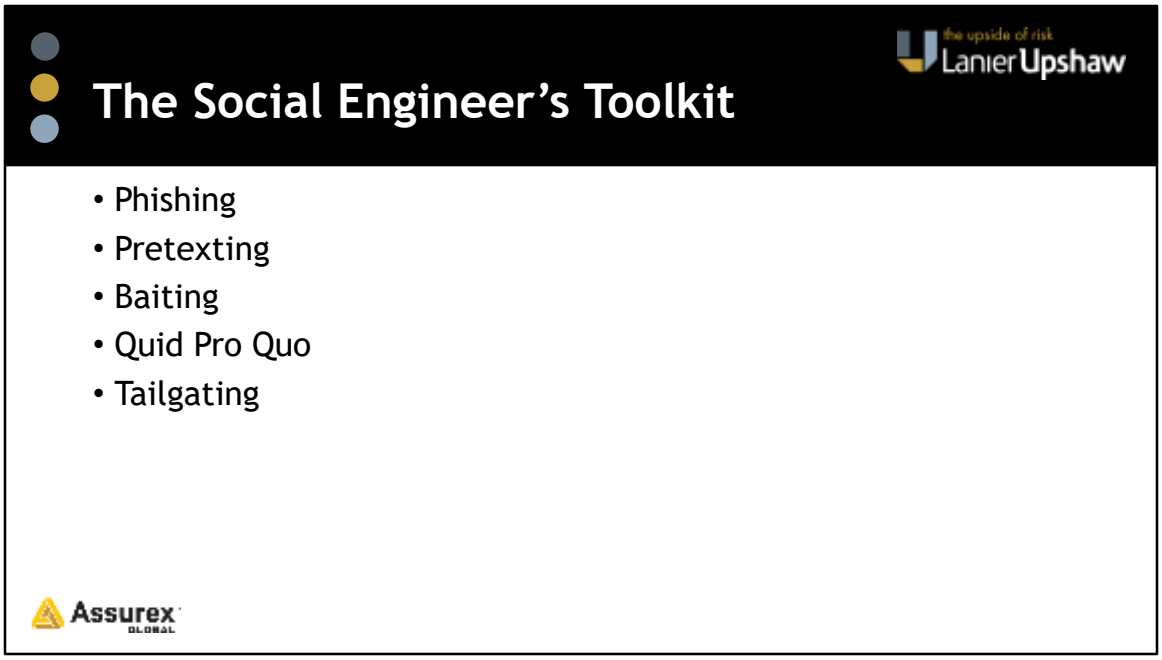
Capture the Flag!

Another mention for the hacking economy - They have a conference every year in Vegas in fact known as BlackHat. The conference participants include the good guys, the bad guys and companies on either side as well.

So back to Social Engineering. It became so prevalent in tactics that it entered the games. There is a long standing contest there known as 'Capture the flag' and a Social Engineering division was started in 2010 at blackhat. In the game of Capture the Flag the rules are explicitly outlined. There are overseeing judges points assigned to meeting certain objectives on the mission.

Participants receive flags a few weeks in advance. In the year of it's inception – targets were all high profile, prominent companies with a goodie bag to grab from. HR, Physical security, facilities, IT. They work via passive information gathering. Looking at your job postings (software you are using, specific skill sets), looking at former employee reviews. Anything that would lend to credibility when in contact with a human on the other end of a phone line.

Social Engineering Tactics



Phishing: Seeks for you to volunteer information. Phishing uses fear and urgency to manipulate their target.

Pretexing: Establishes a fabricated scenario and a false sense of trust to get information from their victim.

Baiting: Free music? Want an iphone?

Quid Pro Quo: similar to baiting but is offering a service. IT assistance, a cheap pen, bar of chocolate, gift card for completing our survey and answering these questions?

Tailgating: Unfortunately, not that kind of tailgating. Following an employee into a restricted area.

Bugs Bunny Anyone?

- Social Engineering is the act of the trickster preying on human psychology, trust, curiosity, desire.

Catch Any Phish Lately?

- 50% of Internet users receive at least one phishing email a day
- 97% of people in the world cannot identify a phishing email
- 1 in 25 actually clicks on the email

- But, however. . . 80% of more than 400 West Point cadets still clicked on a phishing link even after having been subjected to a four hour security awareness training

So the statistics are supportive in indicating that SOMETHING is going to happen at some point to you and/or your company. Super!

But what do we do about it?

Assurex GLOBAL

But what do we do about it?

- Order is:
  - The infrastructure
  - Password Policies
  - Two Factor Authentication
  - Firewalls
  - Putting things in the places we can control
- Identify order:
  - Company Security Policies

But what do we do about it?

- Chaos is:
  - Zero Day vulnerabilities
  - That person who clicked on that email
- Identify chaos:
  - Security Monitoring
  - Security Awareness Programs
  - Employee Training
  - Have an Incidence Response Plan

Hoomans

Working with Employees

- Relevance
- What is in it for them?
- Constant conversations
- Persistent training
- Real-life in the moment dialog

Working as Organization Leaders

- Constant dialog across the organization
  - Top-Down buy in
- IT can't stay in their tower
- Other leaders can't be scared of IT
- Identify your internal 'Targets' (constantly)
- Allow your security strategy to be an ongoing process – just like safety, wellness, etc.
- Learn from incidents
- Don't neglect education – but realize it has to be delivered constantly and in many formats

Resources

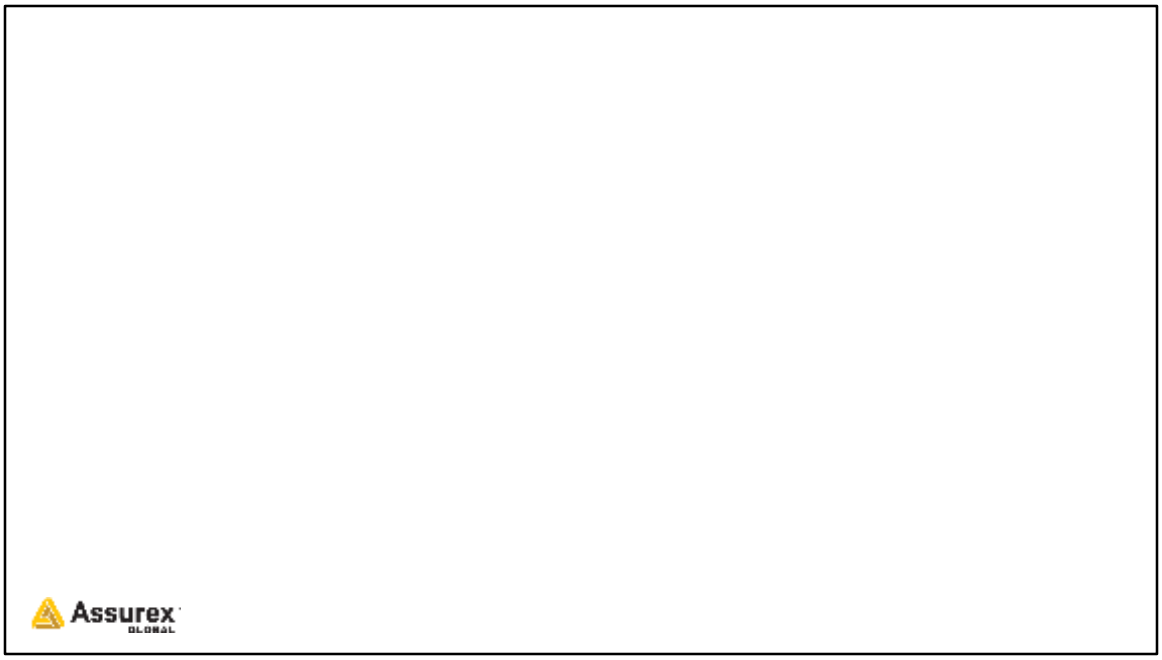
Resources

- Haveibeenpawned.com
  - (assume, yes.)
- KnowBe4
- Last Pass Security Challenge
- Internet Service Providers/Software Vendors
  - Talk to your IT/join them for one of the Security Awareness events!
- Benefits from Cyber Liability Insurance Policies!


the upside of risk
LanierUpshaw
Assurex
GLOBAL


the upside of risk
LanierUpshaw
Assurex
GLOBAL


the upside of risk
LanierUpshaw
Assurex
GLOBAL


Assurex
GLOBAL


the upside of risk
LanierUpshaw
Assurex
GLOBAL


the upside of risk
LanierUpshaw
Assurex
GLOBAL