

Social Engineering & Cyber-Fraud

Dayton Fraud, Cyber, & Ethics Conference
November 6, 2019

James D. Robinson, PhD
Professor of Communication
University of Dayton

The Victim

- Maria Grete
- 62 year old art teacher
- Recent divorcee
- Lives in Sweden
- After a night out on the town, her girlfriends helped her create a profile for an online dating website
- Maria meets Johnny online



Johnny

- 58 year old civil engineer
- Born in South Carolina
- Works in England
- Is a widower
- Has a college age son named Nick
- Johnny has to go to Nigeria for business before he can come to Sweden to meet Maria

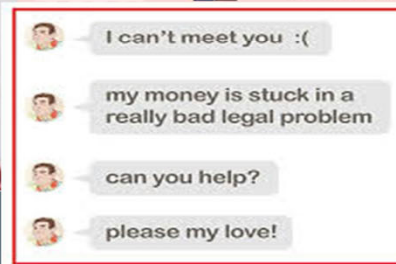
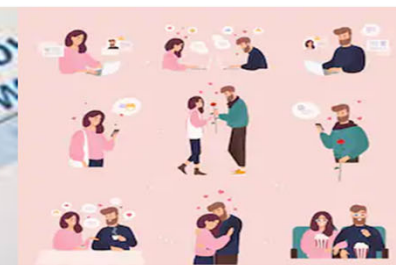


What Happens...

- Johnny texts Maria before the flight takes off
- Johnny & Nick get mugged by their hotel
- Nick gets shot in the face
 - Their wallets are stolen
 - Their identification is stolen
- Johnny contacts Maria in a panic
- Hospital refuses Nick treatment w/o pay
- Johnny's bank has no branch in Lagos, Nigeria
- They desperately need Maria's assistance
- She wires 1,000 € for Nick's surgery



What do you think about Maria?



Online Dating Scams

Has an online love interest asked you for money?

That's a scam.

Bad outcomes

- Many stalkers prey on young persons online
- Person may not be who they claimed to be online
- Always uncertainty/risk
- May be friendly online but different in real life



What my students think about Maria & Johnny

- Maria is old
- Maria is desperately lonely
- I feel sorry for Maria
- Maria is an idiot
- Johnny is a terrible person/predator
- I would never fall for that scam

My Students Fail to Understand Context

1. Context Influences Meaning
 - My brother was reading a book by Mark Twain
2. The Relationship Between Communicants Influences Meaning
 - Having a priest as a graduate student; One Adam Teddy “I know yo’ ...”
3. Memory is susceptible to context changes
 - Remember an embarrassing moment from your childhood
4. All messages contain content and relationship information
 - Teaching at Oklahoma & Gregory Bateson’s dogs

Contextualization is not Automatic or Easy



- The relationship between arousal & attraction
- Arthur Aron study I
- Arthur Aron study II
- Dolf Zillman's study on excitation transfer & misattribution effects

How can Maria Fall for this Scam?

- Uses & Gratifications – Elihu Katz
 - We shape content to meet our needs/we are not disinterested parties in perception
- Self Perception Theory – Daryl Bem
 - Public Commitment strengthens attitudes/she talked about her online boyfriend
- Cognitive Dissonance – Leon Festinger
 - People like to behave consistently with their attitudes/once she declares him her boyfriend
- Norm of Reciprocity – Alvin Gouldner
 - People reciprocate gifts and behavior/he treats her well – she reciprocates
- Foot-in-the-Door – Freedman & Fraser
 - Yard signs/a little bit at a time
- Self Disclosure increases intimacy – Wheeler
- Nonverbal Immediacy

Maria Believed she was in a relationship

- Social Exchange Theory – John Thibaut & Harold Kelly
- We keep track of the rewards and costs in our relationships
 - Rewards – things that fulfill our needs
 - Costs – things that inhibit our behavior
- The value of rewards & costs is determined by our
 - Comparison Level – Relevant Past Relational Experiences/Expectations
 - Comparison Level Alternative – Available Relational Alternatives
- Maria & Johnny Maintain their Relationship today



Relational Outcome Matrix

My Relationship ...	No Superior Relational Alternative (REL is stable or unstable)	Superior Relational Alternative Available (REL is stable or unstable)
Fails to meet CL Expectation (Satisfying or Unsatisfying)	Your relationship is Unsatisfying & Stable	Your relationship is Unsatisfying & Unstable
Exceeds my CL Expectation	Your relationship is Satisfying & Stable	Your relationship is Satisfying & Unstable

Maria's Story is not that surprising...

- In 2018, nearly 18,500 individuals reported to the FBI that they were victims of an online dating scam.
- Whitty (2017) surveyed 11,780 people (volunteer sample) from UK.
 - 728/10,723 were one-off victims (7%)
 - 329/10,723 were repeat victims (3%)
 - 200/10,723 of the victims were victims of a romance scam (1.8%)
- The following characteristics were associated with being victimized
 - Impulsivity, Kindness, Trustworthiness, Trust in others, Locus of control, Greed & Addictive personality characteristics
 - Self reported knowledge cybersecurity knowledge was inversely related to victimization.
 - Education level was also inversely related to victimization
 - Middle age (35-54) more likely to be scammed than young (18-34) and older (55+)

What We Know About Phishing Tests at UD

- Everyone falls for the right message
- 20% faculty & staff fall for an Amazon phishing message
 - Goes up dramatically near Christmas
- Faculty don't fall for purchase order phishing messages
 - People in purchasing do fall for them
- Faculty fall for phishing messages if the hacker asks for a copy of their research
 - Faculty will contact Udit and complain that they can't send a pdf to someone – even after the “this is a phish” educational message appears
- A quick history lesson – George C. Parker sold the Brooklyn Bridge several times
 - Police had to stop the buyers from setting up toll booths
- He also sold the Statue of Liberty, Grant's Tomb, Madison Square Garden, & the Metropolitan Museum of Art

New Realities of Cybersecurity

1. We can't solely **"engineer" our way to comprehensive cybersecurity**

But we must continue innovating with technologies that better monitor, predict and protect.

2. We can't solely **rely on central command & control to enforce effective cybersecurity**

But we must continue establishing and enforcing best practices

3. We can't **achieve highly reliable cybersecurity solely through compliance-focused education programs**

But we must ensure continuous & engaged learning

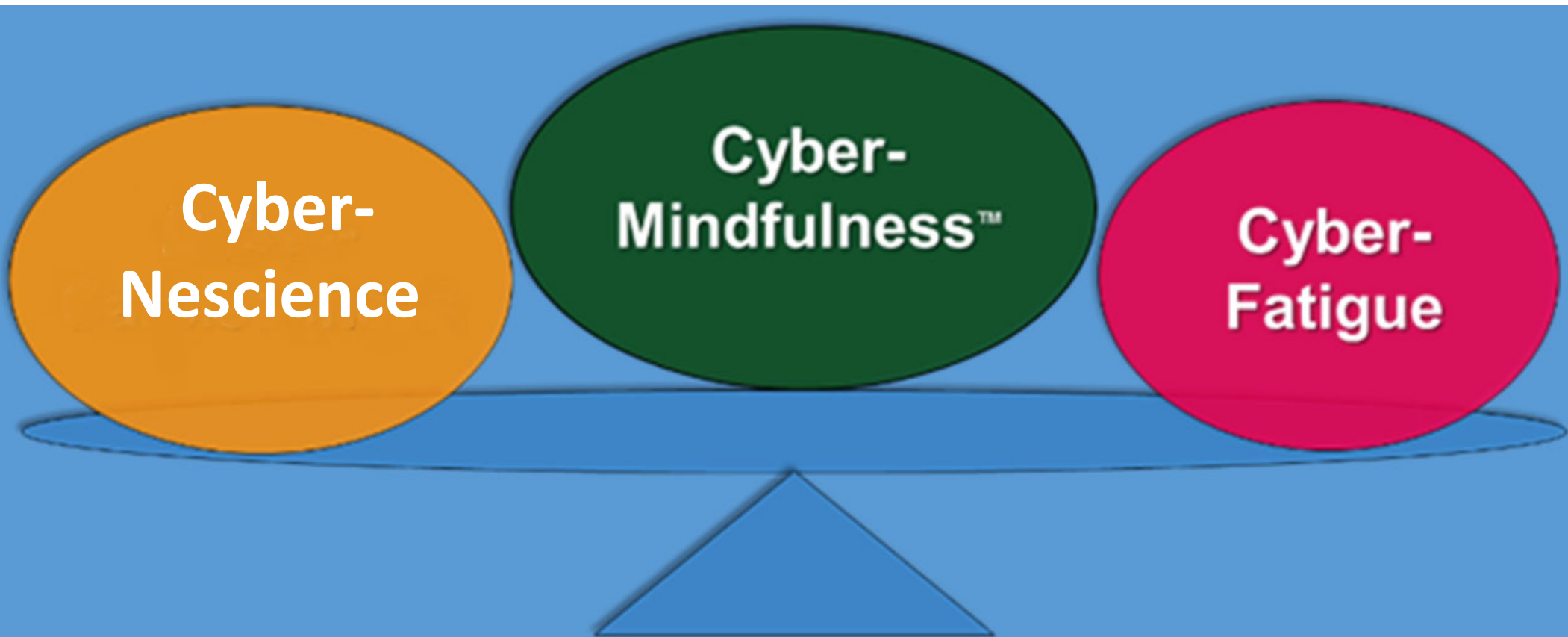
4. *We must make end users cyber-mindful*

Ellen Langer Mindfulness & Mindlessness

Classic Study on Mindlessness

- Most famous study on people processing information mindlessly was conducted by Ellen Langer.
 - Langer's waited until there was a line at the Xerox machine in the library.
 - Her confederate walked up to the people in the line and requested that they be allowed to make their copies first – and not wait in the line.
 - The confederate said to the people in line
 - “Excuse me, I have 5 pages. May I use the Xerox machine, because I’m in a rush?” (94% success)
 - “Excuse me, I have 5 pages. May I use the Xerox machine? (60% success rate)
 - “Excuse me, I have 5 pages. May I use the Xerox machine, because I have to make copies?” (93% success)
- What is the point?
 - Any reason if things are not important is good because they process info mindlessly.

The Cybersecurity “Engagement Fulcrum”



Cybersecurity Fulcrum of Engagement

- We must move people from cyber-nescience to cyber-mindfulness.
- But we can't move them too far or they become cyber-fatigued,
 - Then our messages fall on deaf ears
- We can't legislate morality and we cannot force people into being cyber-mindful or more aware of cybersecurity issues.
 - We need to lead them to reframing cybersecurity from being something they do to protect themselves to something they do to protect others
 - We need to lead them to understand that they do not need to be experts to be mindful of attack vectors
 - All they need to do is become aware of things that are not normal or typical
 - And they need to contact someone in IT at the very moment they notice it
 - Our training will contain information but is focused on keeping people mindful

Comparison of Training Methods for Avoiding Phishing Attacks: Rules-Based vs. Mindfulness-Based Practices*

Rules-Based Practices

1. Never click a link or open an attachment from an unknown sender.
2. Access websites by manually entering the URL.
3. Do not reply to emails asking for private information.
4. Be suspicious of websites requesting sensitive data.
5. Look for browser cues such as HTTP & “lock” icon to identify fake websites.

Mindfulness-Based Practices

1. **Stop**
 - Consider the consequences
 - Avoid “routinized” replies
2. **Think**
 - Does the request ask for private or proprietary information?’
 - Is the request unexpected or urgent?
 - Does the request make sense?
 - Why would the sender need me to do this?
3. **Check**
 - If anything seems suspicious, verify the request with a trusted third party.

*Jensen, Matthew L., et. al. (2017) “Training to Mitigate Phishing Attacks Using Mindfulness Techniques.” *Journal of Management Information Systems*. Vol. 34, No.2, pp. 597-626

Becoming Cyber-Mindful™

Awareness

- Awareness of personal & institutional risks online.
- Continuous learning about exploits & threats.
- Knowledge of ways to respond to dangers.

"I know that cybersecurity threats are real, persistent & dangerous."



Agency

- Attitude of personal efficacy in defending against shared risks.
- Acceptance of shared responsibility in protecting information.
- Confidence that personal actions can make a difference.

"I believe that these risks are important & meaningful to me & I can do something."



Action

- Behavioral habits align with scale of threats.
- Alertness to potential threats leads to appropriate preventive & defensive actions.
- Engagement results in regular communication with peers & IT regarding potential risks

"I will take actions to reduce risks to me & my organization – & I have practiced them!"

To increase cybersecurity we must

- Help the people in IT have to develop relationships with the end users
 - Not best friends but the kind of professional relationships that allow people to feel like they can ask for help and provide help to others
- Use of “controlling” or “dogmatic language” increases the likelihood of a reactance responses
 - Unfortunately messages intended to produce behavior change often feel like restricted and not free choice
 - The only thing you can do is change the relationship between IT professionals and end users
- People cannot be embarrassed or afraid to signal a problem or to indicate they have been victimized

We have to understand the use of Fear Appeals

- The problem is that fear appeals produce two different effects
 - When fear produces a Danger Control response, we change our behavior because we believe it will keep us from becoming a victim
 - When fear produces a Fear Control response, we denigrate the source and the information to avoid feeling fearful
- What determines the outcome of fear producing messages is
 - Response Efficacy (I believe the proposed solution will work)
 - Self-Efficacy (I believe I can successfully enact the solution)
- Fear without efficacy just doesn't work
- Our training has to produce increased efficacy – even if it is just call IT and email your friends you became a victim or noticed a strange email

Actual Social Engineering

- I get my bottled water from a place in Enon.
- I treat the young women nice & act interested in them.
- All day they remind people about water deliveries & leave phone messages
 - So I ask them – how many calls they make a day?
- One day I give the woman a few dollars for a bottle of water. One of the bills has a small cat punched out of it
- She loves cats and wanted to save the dollar for herself. She starts looking in her purse for a dollar to replace it and I pull one out of my pocket and give it to her.
- 3 weeks later she says “I am taking another job – so I might not see you again.
- I thanked her for taking care of me, asked about her cat & then her new job

The Cat's Meow

- She told me that she took a job at P&C Bank & starts the following week.
- I don't know which branch but I bet it's within 20 minutes of Aqua Falls
- I could open an account at that branch & maintain our relationship.
 - Could I get her to give me the combination of the safe?
 - No but I bet I could get inside information I could use for spear phishing
 - She told me that the new owners alienated everyone so much they all quit
 - Company is not publicly traded so the information was no good to me
- If I were a real showman, I would pull out a hole punch & punch a cat shape out of a dollar bill for you – but I have no idea who punched the cat out of the dollar.
- I am not a stalker – I am a student of human behavior.

The End

Inattention Blindness

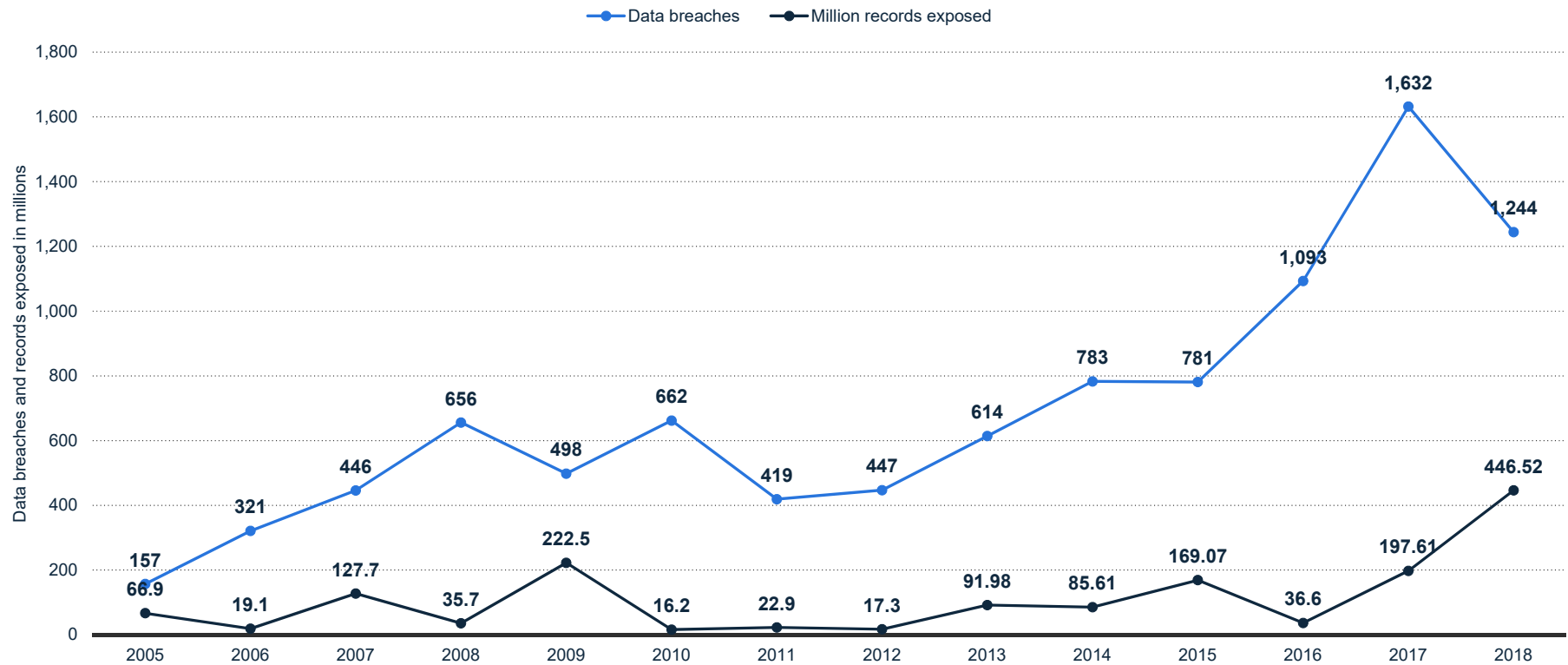


- if we are paying very close attention to one thing, we often fail to notice other things in our field of vision— even very obvious things.



Number of data breaches & exposed records U.S. 2005 –2018

Cyber crime: Number of breaches and records exposed 2005-2018 in millions



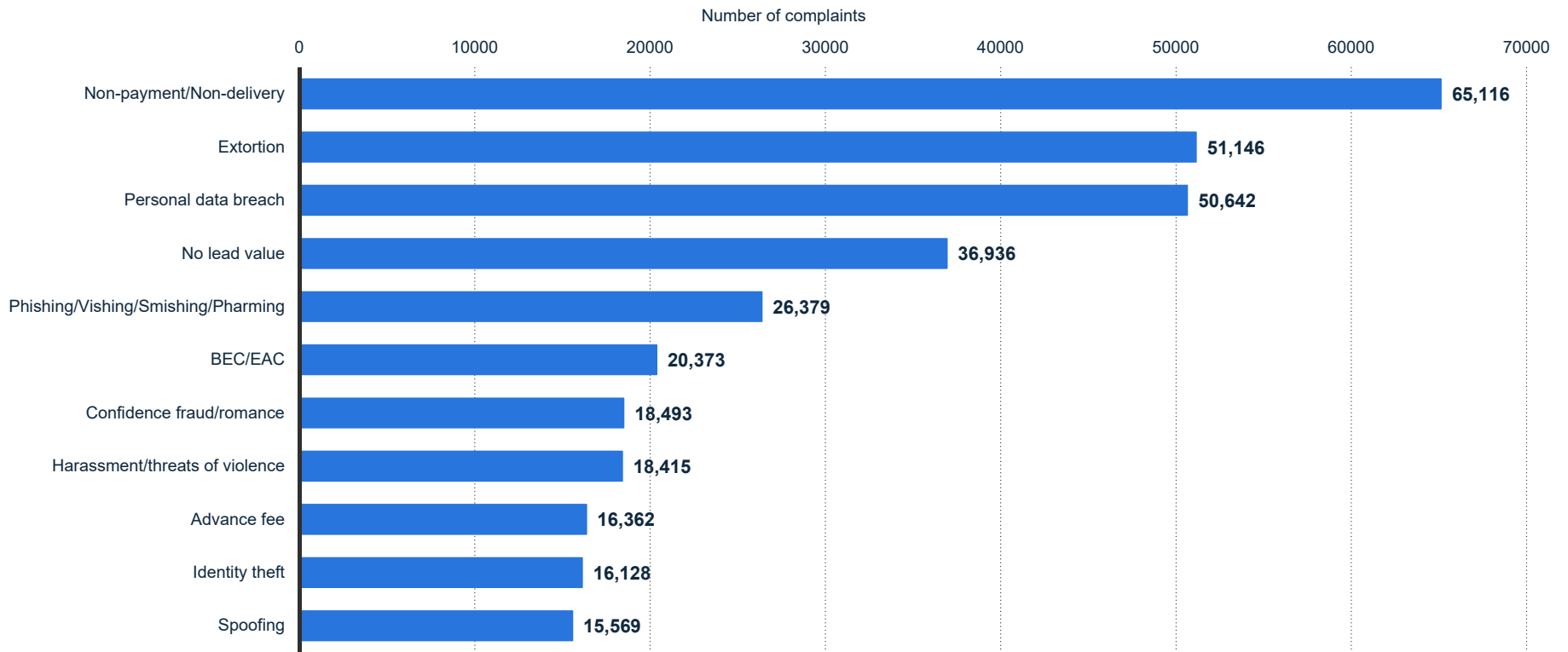
Source(s): Identity Theft Resource Center; [ID 273550](#)

11/4/2019

The Real McCoy

Types of cyber crime most frequently reported to the IC3 by victim count

Most commonly reported types of cyber crime 2018



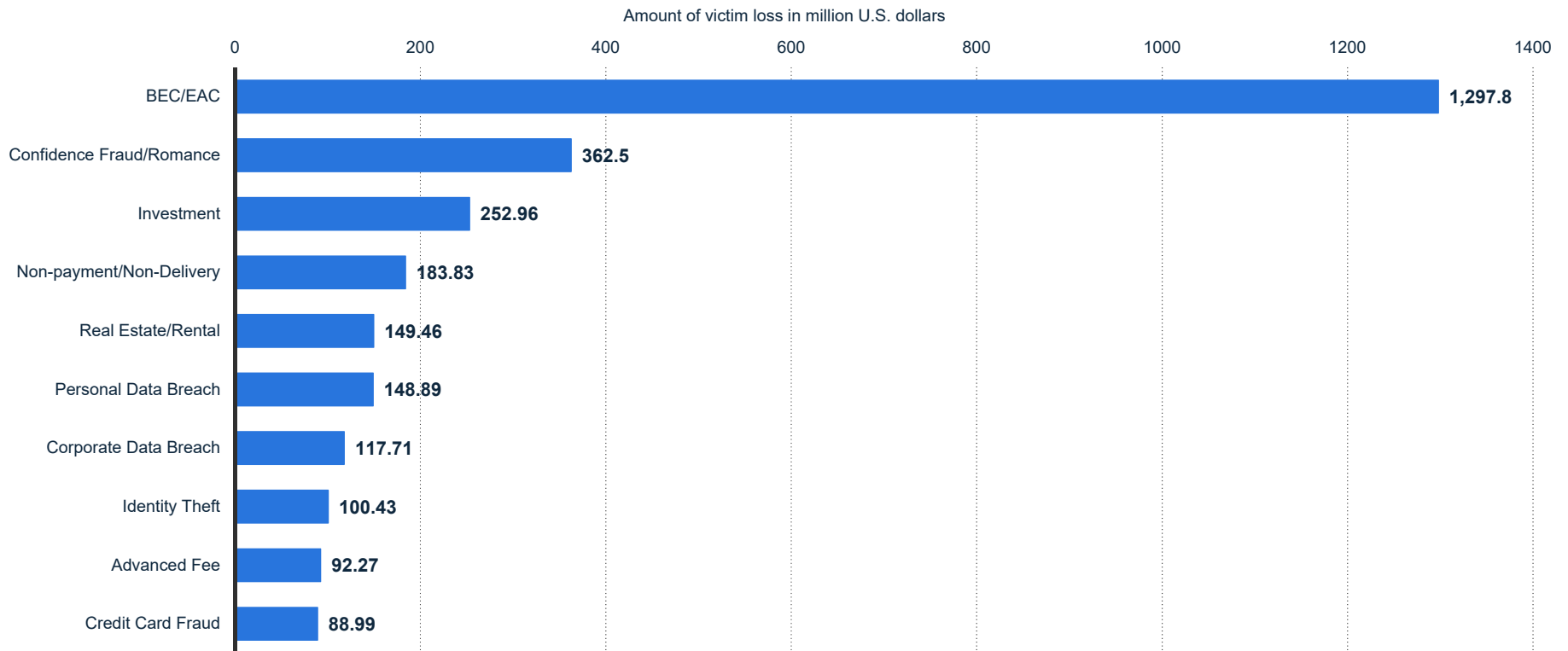
Source(s): FBI Internet Crime Complaint Center (IC3) [ID 184083](#)

11/4/2019

The Real McCoy

Cyber crime with the highest amount of victim losses in 2018

Leading cyber crime victim loss categories 2018 in millions of U. S. Dollars



Source(s): FBI Internet Crime Complaint Center (IC3) [ID 234987](#)

The Real McCoy