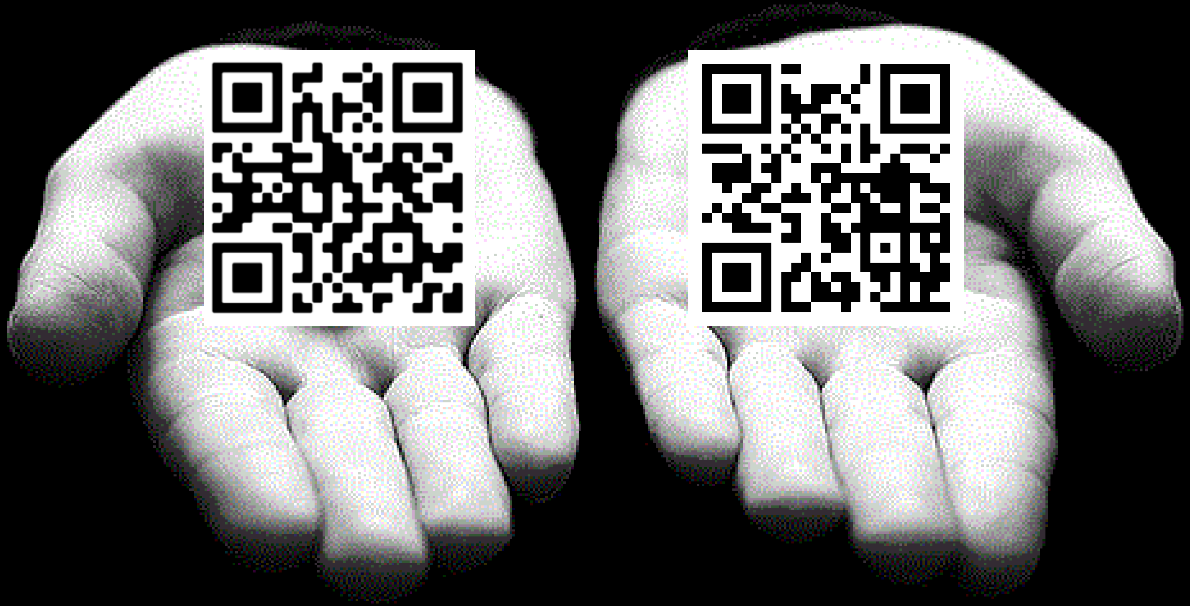
M&T Tech

Choose wisely:
One will check you in to the talk
The other is good for a laugh



Win Friends, Influence People, Hack Them

Exploiting Humans through Social Engineering (V3)

Taylor Kaufman, CISSP; Advanced Threat Hunter

M&T Tech

Quick disclaimer

- This presentation is intended for educational purposes only and do not replace independent professional judgement. Statements of fact and opinions expressed are those of the presenter individually, and, unless expressed stated to the contrary, are not the opinions or positions of M&T Bank
- This presentation aims to tell you examples, historical events, and studies of cybersecurity with a focus on social engineering and psychology
- DO NOT TRY EXAMPLES IN THIS PRESENTATION WITHOUT FIRST HAVING CONSULTED AND OBTAINED WRITTEN PERMISSION. There are real legal ramifications to ‘hacking’, even if done with teaching or other ‘good’ intentions in mind.
- The presenter cannot be held responsible if you decide, despite disclaimer, to attempt social engineering attacks on your own accord

About Me

Current Role

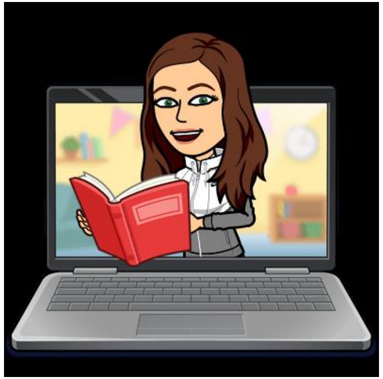
- **Advanced Threat Hunter, M&T Bank**
- **CISSP, MS Azure Fundamentals, Network+, Security+ certified**

Previous roles

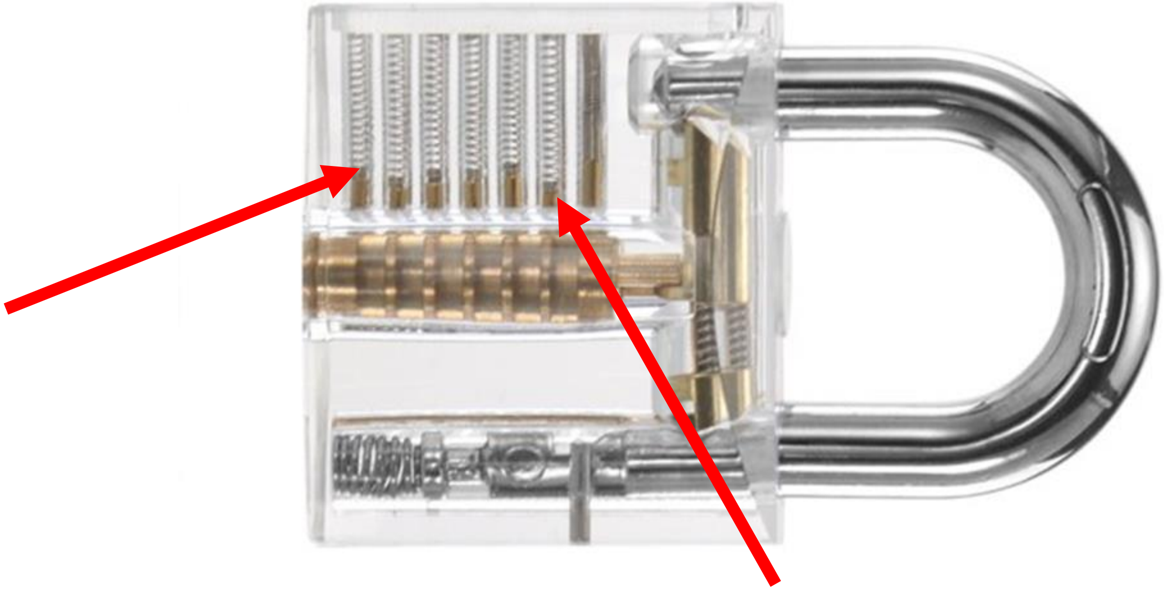
- **2.5 years - Risk process technical specialist III, M&T**
- **2.5 years - Security Engineer, Seneca Gaming**
- **1 year - IT support technician, Seneca Gaming**

Personal

- **Graduated Buffalo State College class of 2015**
  - B.S. Computer Information Systems
  - B.A. Television/Film arts
  - Minor, Philosophy
- **InfraGard Buffalo and Technology advisory board member for the town of Grand Island**
- **Amateur boxer out of Casal's boxing club**
- **Rucker (GRT & M&T VRG corporate liaison for the KIA memorial Roadmarch)**



{Cybersecurity} as a Lock



Cybersecurity code of ethics

Code of Ethics Canons (ISC2):

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

1. Protect society, the common good, necessary public trust and confidence, and the infrastructure.
2. Act honorably, honestly, justly, responsibly, and legally.
3. Provide diligent and competent service to principals.
4. Advance and protect the profession.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."
-Sun Tzu, The Art of War

What is Social Engineering?

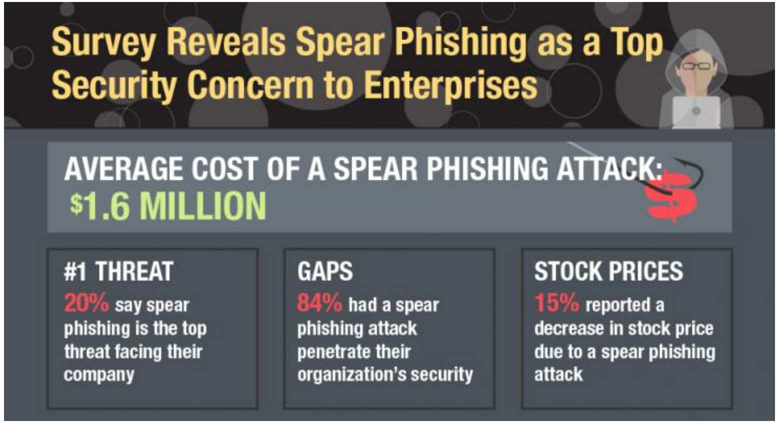
Fact: This isn’t your Nigerian Prince Scam anymore

SE: Any act that influences a person to take an action that may or may not be in their best interest.

Top attack vectors:

1. Phishing - Emails
2. Vishing – Phone calls
3. Impersonation – Pretexting as another person
4. Smishing - Text messages

Well, Lois, the truth is I'm actually Superman in disguise.
I only pretend to be a journalist to hear about disasters as they happen and cut you out of the byline.



Survey Reveals Spear Phishing as a Top Security Concern to Enterprises

AVERAGE COST OF A SPEAR PHISHING ATTACK: $1.6 MILLION

#1 THREAT
20% say spear phishing is the top threat facing their company

GAPS
84% had a spear phishing attack penetrate their organization’s security

STOCK PRICES
15% reported a decrease in stock price due to a spear phishing attack

Goals of a malicious SE:

- The goals of a malicious SE are comparable to the goals of any criminal activity.
- Ex. Knowledge, Power, Money, Control, Bragging rights, etc.

Goals of ethical Social Engineering:

- Test current security controls to ID potential gaps
- Offer suggestions to improve security

Notable historical events of social engineering

1894: J.C. Van Marken introduces the term “sociale ingenieurs”

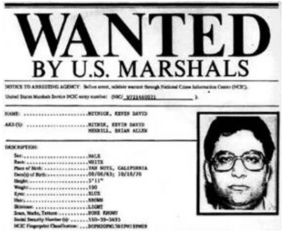
1960s Frank Abagnale, Pan-Am “catch me if you can”

Modern 2000s: Phishing, Vishing, Faxing, etc. pick up steam

1184 BC Trojan Horse

1920s Charles Ponzi scheme

1990s Kevin Mitnick, “The art of deception” One of the most wanted SEs



WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID
AKA(S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number(s): 330-39-3695
NCIC Fingerprint Classification: ...[illegible]

Today: War, media, and politicians use social engineering to sway public opinion with social campaigns, etc.

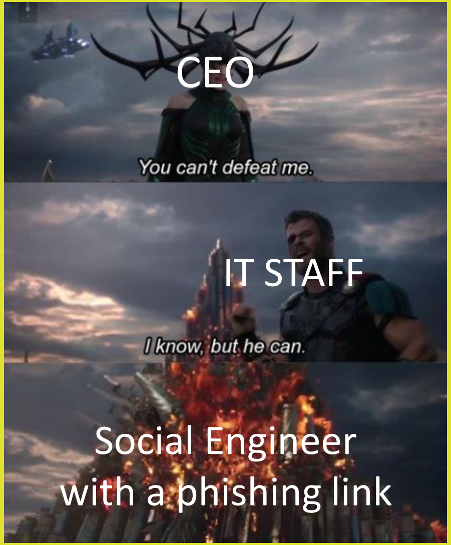
True Story

The Target:

- The target was a decent-sized printing company in the U.S. that had some proprietary processes and vendors that some of its competitors were after.
- The IT and security teams realized the company had some weaknesses and convinced the CEO an audit was needed.
- The CEO arrogantly said that he knew that "hacking him would be next to impossible because he guarded these secrets with his life." Not even some of his core staff knew all the details."
- CEO held tons of important company secrets solely on his laptop.

Steps:

-OSINT – found email of CEO by using style of other employees.
-Used a tool (Maltego) to find a previously closed invoice (sponsor package).
-SE as an employee to find what the venture invoice was from.
-Dug into the CEO and the charity event using basic internet searches
-Called marketing director of company while pretending to be from the charity event and gathered more information that way
-Planned attack vector using the charity as a front and a malicious PDF containing all the info.



M&T Tech

True Story

END RESULT:
Armed with the information, SE called the CEO and posed as a fundraiser from a cancer charity the CEO had dealt with in the past. He informed him they were offering a prize drawing in exchange for donations--and the prizes included tickets to a game played by his favorite sports team, as well as gift certificates to several restaurants, including his favorite spot.

The CEO agreed to let the SE send him a PDF with more information on the fund drive. He even managed to get the CEO to tell him which version of Adobe reader he was running because, he told the CEO "I want to make sure I'm sending you a PDF you can read." Soon after he sent the PDF, the CEO opened it, installing a shell that allowed the SE to access his machine.

Takeaway 1: No information, regardless of its personal or emotional nature, is off limits for a social engineer seeking to do harm

Takeaway 2: It is often the person who thinks they are the most secure who poses the biggest vulnerability. Executives are the easiest social engineering targets.

Other true examples of social engineering

Ransomware Gangs

Salesmen/women

Malicious/Fake apps

Politicians!

Frank Abagnale aka "Catch Me If You Can"

Victor Lusting aka "The Man Who Sold The Eiffel Tower"

George Parker aka "The Man Who Sold The Brooklyn Bridge"

"The Tinder Swindler" Simon Leviev/Shimon Hayut

Bernard Madoff "Nigerian Prince" 'Influencers' pushing new crypto

The ‘Good Guy’ social engineer

The Social Engineering Code of Ethics accomplishes these three important goals:

- Promotes professionalism in the industry.
- Establishes ethics and policies that dictate how to be a professional SE.
- Provides guidance on how to conduct a social engineering business.

“Leave Others Feeling Better For Having Met You”

Social engineering village at DefCon

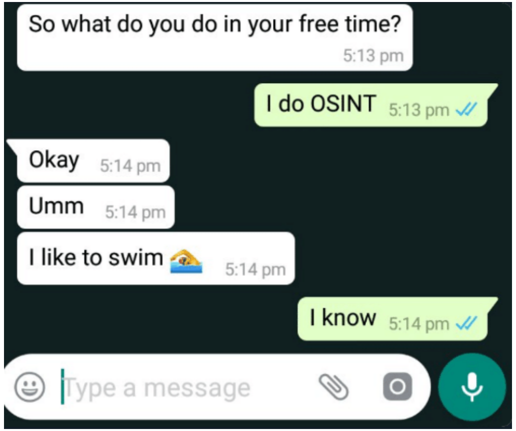
Social Engineering Ex.

And I can't remember what email address
we used to log on to the account,
and the baby's crying-

Scenario: What would you do?

Social Engineering Attack Cycle

1. Information Gathering (OSINT)
2. Establish Relationship and Rapport
3. Exploitation
4. Execution



So what do you do in your free time? 5:13 pm

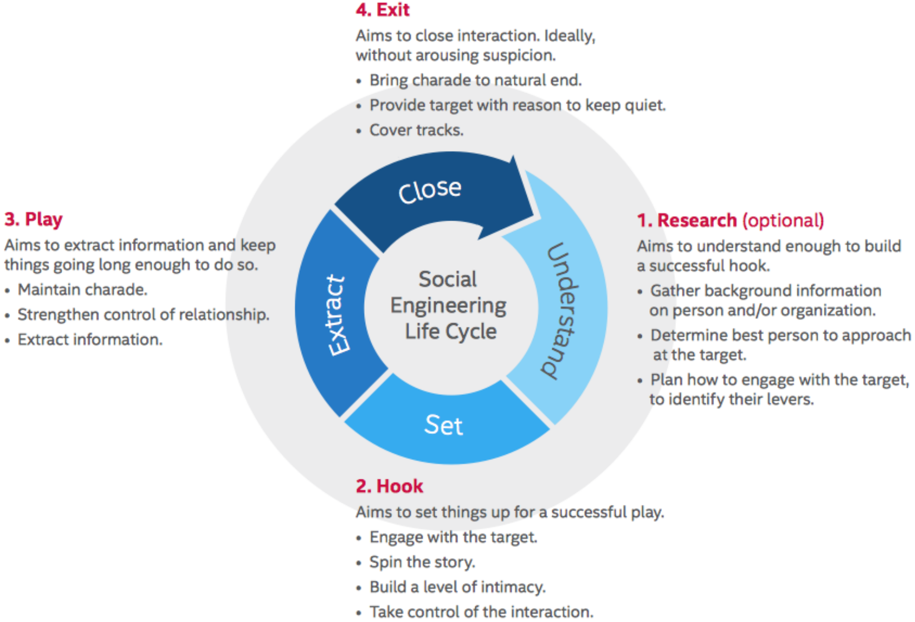
I do OSINT 5:13 pm

Okay 5:14 pm

Umm 5:14 pm

I like to swim 🏊 5:14 pm

I know 5:14 pm



4. Exit

Aims to close interaction. Ideally, without arousing suspicion.

- Bring charade to natural end.
- Provide target with reason to keep quiet.
- Cover tracks.

3. Play

Aims to extract information and keep things going long enough to do so.

- Maintain charade.
- Strengthen control of relationship.
- Extract information.

1. Research (optional)

Aims to understand enough to build a successful hook.

- Gather background information on person and/or organization.
- Determine best person to approach at the target.
- Plan how to engage with the target, to identify their levers.

2. Hook

Aims to set things up for a successful play.

- Engage with the target.
- Spin the story.
- Build a level of intimacy.
- Take control of the interaction.

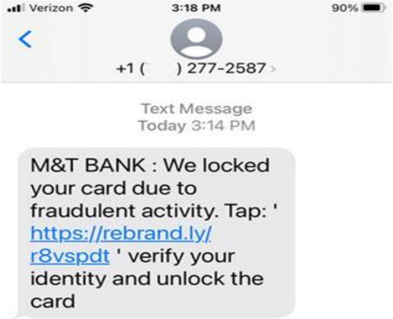
The four phases of a social engineering attack.

How do we protect ourselves from social engineering?

Spot the scam

People are the target and line of defense—learn how to recognize SE attacks.

If you're unsure—report it!

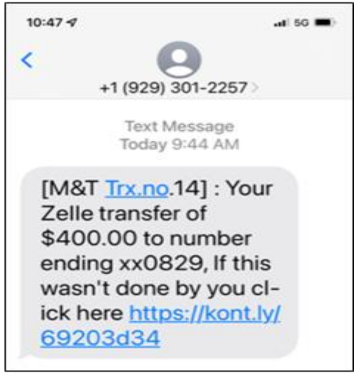


Verizon 3:18 PM 90%

+1 (   ) 277-2587

Text Message
Today 3:14 PM

M&T BANK : We locked your card due to fraudulent activity. Tap: ' https://rebrand.ly/r8vspdt ' verify your identity and unlock the card



10:47 5G

+1 (929) 301-2257

Text Message
Today 9:44 AM

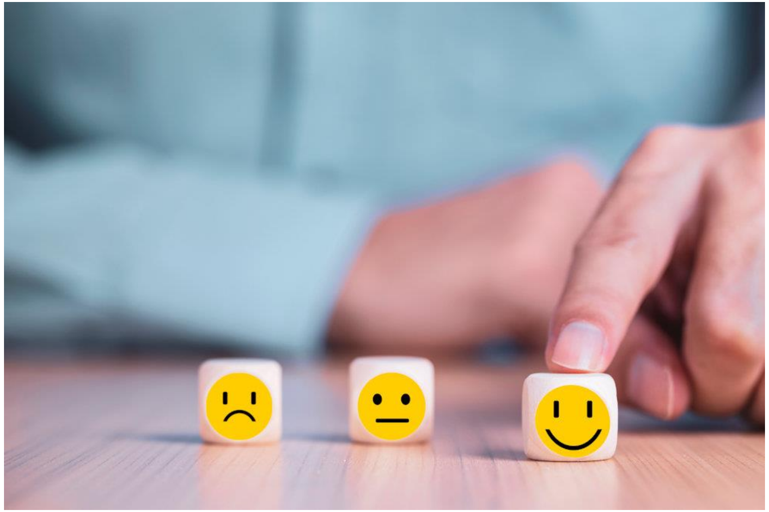
[M&T Trx.no.14] : Your Zelle transfer of $400.00 to number ending xx0829, If this wasn't done by you cl-ick here https://kont.ly/69203d34

Using social engineering to your advantage

Building Rapport to make your job easier

1. Using artificial time constraints
2. Accommodating nonverbals
3. Use a slower rate of speech
4. Employ sympathy or assistance themes
5. Suspending your ego
6. Validating others
7. Asking how, why, and when questions
8. Making use of quid pro quo
9. Employ reciprocal altruism
10. Managing expectations

Learning Social engineering helps your awareness of self and others



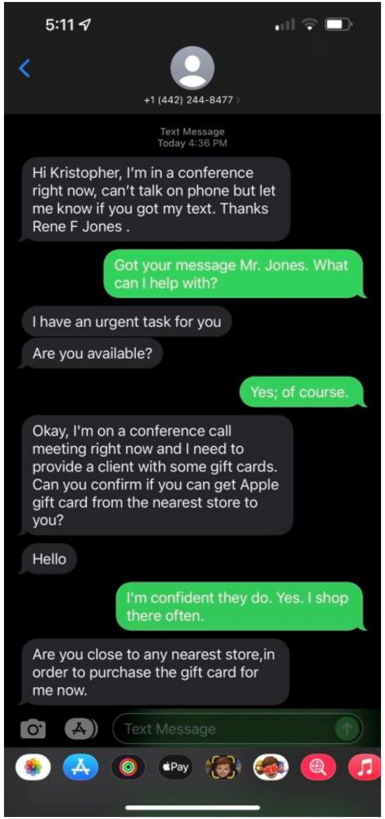
Be conscious of what information you put out publicly on social media, what usernames and passwords you repeat elsewhere, etc.

Using social engineering to your advantage pt. 2

!Do not troll if you are not experienced in dealing with malicious actors!

There are several YouTube channels out there ‘hacking’ or taking down scammers. Entertainment value of SE is fun but be careful of legal ramifications of “scamming back”!

The screenshots are an example of legal and ‘safe’ SE



Hi Kristopher, I'm in a conference right now, can't talk on phone but let me know if you got my text. Thanks Rene F Jones .

Got your message Mr. Jones. What can I help with?

I have an urgent task for you

Are you available?

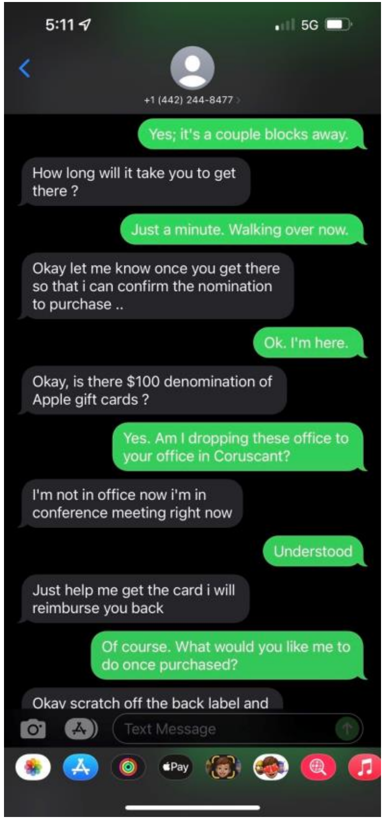
Yes; of course.

Okay, I'm on a conference call meeting right now and I need to provide a client with some gift cards. Can you confirm if you can get Apple gift card from the nearest store to you?

Hello

I'm confident they do. Yes. I shop there often.

Are you close to any nearest store,in order to purchase the gift card for me now.



Yes; it's a couple blocks away.

How long will it take you to get there ?

Just a minute. Walking over now.

Okay let me know once you get there so that i can confirm the nomination to purchase ..

Ok. I'm here.

Okay, is there $100 denomination of Apple gift cards ?

Yes. Am I dropping these office to your office in Coruscant?

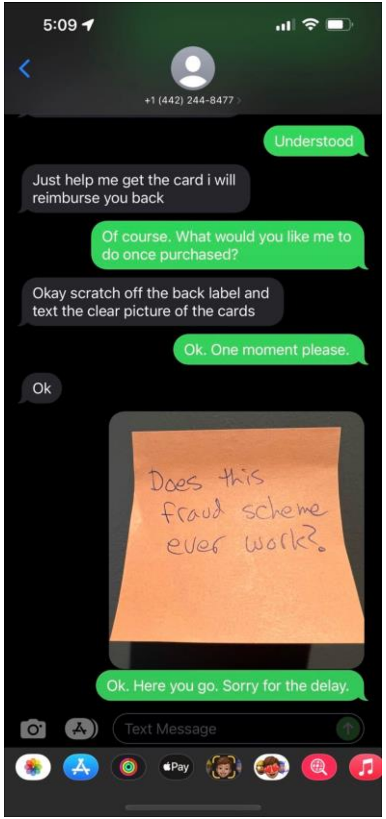
I'm not in office now i'm in conference meeting right now

Understood

Just help me get the card i will reimburse you back

Of course. What would you like me to do once purchased?

Okay scratch off the back label and



Understood

Just help me get the card i will reimburse you back

Of course. What would you like me to do once purchased?

Okay scratch off the back label and text the clear picture of the cards

Ok. One moment please.

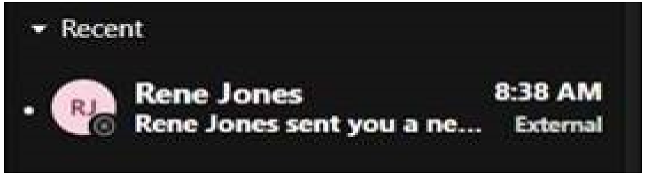
Ok

Does this fraud scheme ever work?

Ok. Here you go. Sorry for the delay.

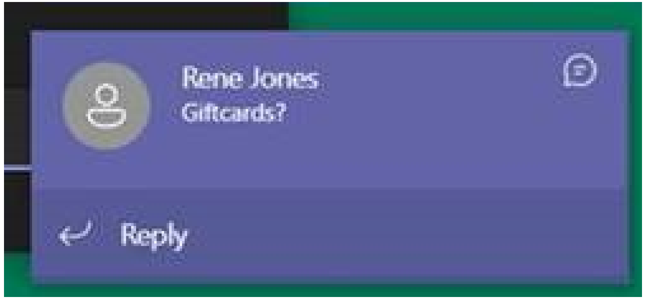
What are the cyber folks doing to protect M&T?

{Think like a bad guy. Pretend to be bad guy. Build defenses to stop the bad guy}



Rene Jones 8:38 AM

Rene Jones sent you a ne... External



Rene Jones

Giftcards?

{Stop them from getting to people where we can}

Proactive defense: Content filters, threat intelligence, responsible disclosure, crawling public repositories (ex. github), vendor searching 'darknet' domains, external pentests, and security awareness training

Reactive defense: Phishing domain takedown efforts and collaboration with other teams (like Fraud).

Other: **YOU!** We are all responsible for cybersecurity. Congratulations on your new cybersecurity gig.

Under certain conditions (aka with written approval), it is ok to pretend to be the bad guy when testing controls.

HOWEVER:

Please, do not try to attempt malicious activities on M&T devices—you will raise incident response action.

Please do not make physical security's lives more difficult by trying to break into areas you do not belong in

Please do not make the help desk worker's lives more difficult by trying to access accounts that are not yours.

Please do not make your manager's life more difficult by having them have to explain why you attempted something that goes against moral judgement and character

If you happen to notice something that seems off or might warrant further testing, feel free to reach out to us!

If you are afraid that you may have been the victim of a social engineering attack (phishing, smshing, etc.) please reach out to csoc@mtb.com as soon as possible

Questions?

"Sorry, I wasn't trying to summon you—I was just trying to pull up the ~~menu~~ Check in *on my phone."*

If you were too
nervous before, again,
here is the check in link

M&T Tech