

Overlay Network Threats (eg Social Media)

UT LAW396V

SPRING 2023

LECTURE NOTES



Overlay Networks

Any network overlaid on top of another

Network Requirements:

- 1. Bootstrap (initial access)
- 2. Addressable
- 3. Routable
- 4. Data Transfer

Example: Social Media Networks (including Email)

The Power of Socially Connected Networks

Social networks are ***semantic***

Networking is tied to human psychology

- 1. Bootstrap – friends, company, identity
- 2. Addressable – social connections
- 3. Routable – social graph (e.g., friends of friends)
- 4. Data Transfer – psychological investment

Social Network Vulnerabilities

Users import emotions/beliefs into the network

Users traffic in vitally important information

None of our “perimeter defense” applies

Attackers can directly attack the psychology surface

Attackers have valuable data

Common Attack Types:

Personal Theft or Fraud

Organization Theft or Fraud

Destruction of Reputation

Threat Category	Threat actors and motivations	Impacts
Theft and financial fraud targeting customers and third parties	Cybercriminals: Financial gain	Indirect: Damage to reputation; Loss of sales Direct: Resolution of disputes
Attacks on reputation	Hactivists: Ideology or politics Disgruntled customers and employees: Anger or revenge	Indirect: Damage to reputation; Loss of revenue Direct: Costs to counter misinformation
Attacks against the enterprise and employees	Cybercriminals: Financial gain Competitors and state actors: IP and embarrassing information	Indirect: Damage to brand; Loss of competitive position Direct: Breach notification costs; regulatory fines; disruption of operations

Source: "A Taxonomy of Digital Threats"
Zero Fox Corporation

Email Threat: SPAM

You know what it is.

Why does it work?

- Advertising
- Pump and Dump
- Malicious Payload/Malicious Links
- Unregulated/Illegal Traffic

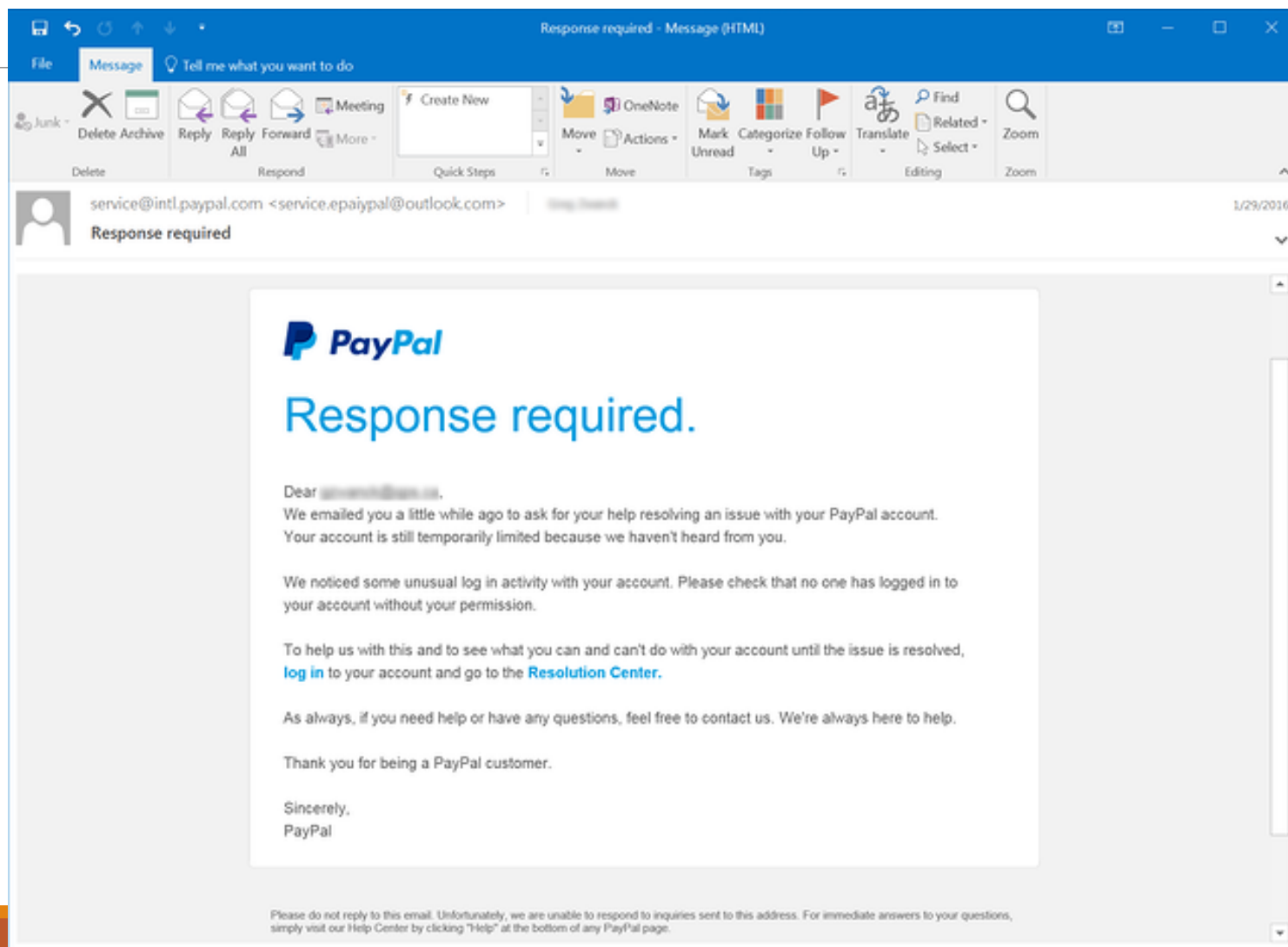
Spam Incentives

It costs virtually nothing to send emails

- It costs the same to send 1 message vs 1 million
- Many spam messages are sent by botnet

BULK messages: Less than 1% response rate is great

Email Threat: Phishing



Bulk Phishing Concepts

Psychology

- Visually, looks authoritative
- Urgency drives immediate behavior
- Some phishing is very emotional

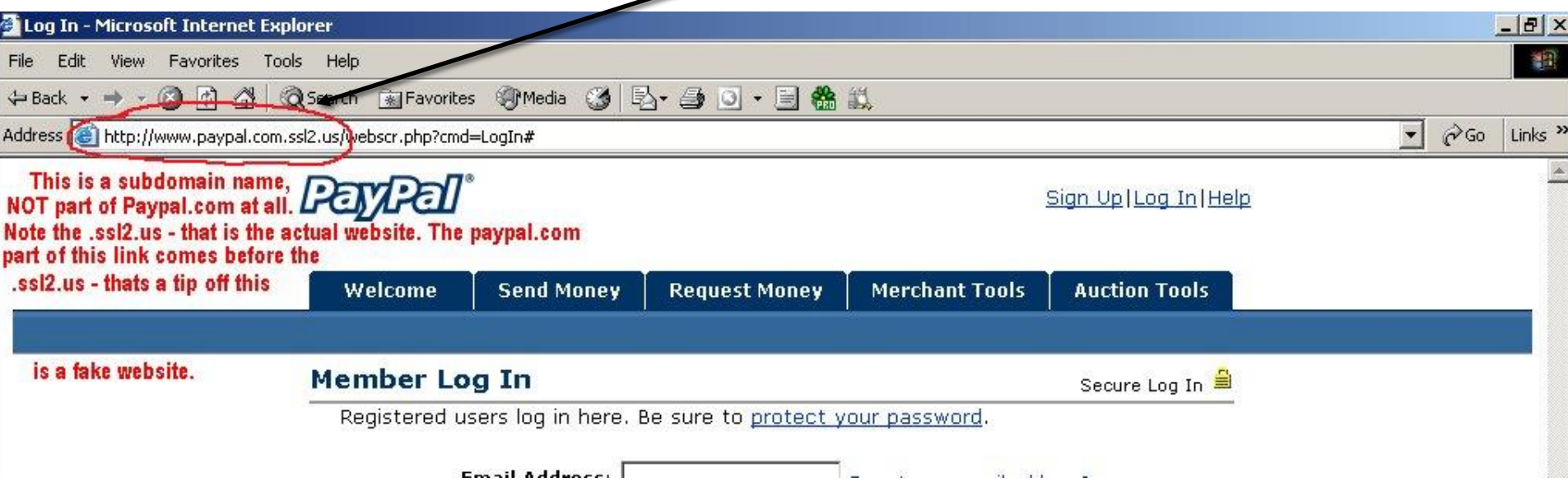
“Call to Action”

- Typically, email response not desired
- Includes either a bad link or malicious attachment
- Bad link goes to fake website that looks real

BULK messages: Less than 1% response rate is great

Phishing Links

Why do they need a fake URL?



Cloud Services as Links

Many phishing emails now use cloud service links

Amazon, Azure, etc. links are not blocked

Also, seem authoritative

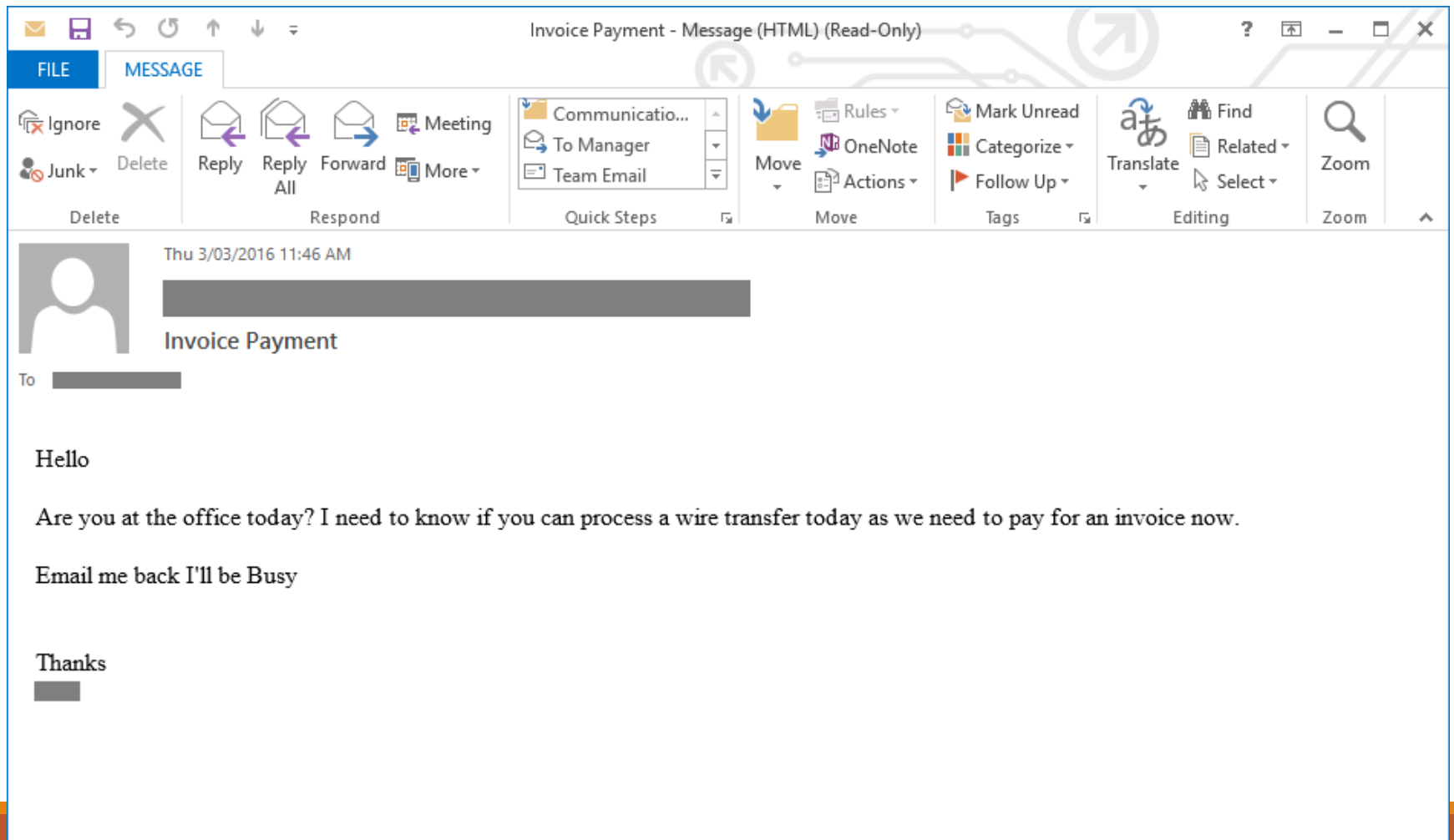
Note About Phishing Training

I've yet to see it work.



Lots of companies try. Lots of products.

Word on the street is the users don't learn

Spear Phishing Example 1



Spear Phishing Example 2

  **Re: Request**

David MacKinnon

Sent: Wednesday, September 16, 2015 at 4:47 PM

To: Rohyt Belani


Cc: Samuel Hahn

Rohyt,
I'll get this done ASAP. Do you want the funds in dollars or GBP?
Thanks,
Dave

Sent from my iPhone

On Sep 16, 2015, at 4:41 PM, Rohyt Belani <rohyt.belani@phishme.com> wrote:

The details are below. Let me know once it has been processed.

Bank Name : Raytown-Lee's Summit Community Credit Union
Bank Address : 10021 E 66th Ter, Raytown, MO 64133
Bank phone number : 816-356-1452
Name On Account : Robert Lee Koerner
Account Number : 
Routing Number : 
Home Address : 6553 Raytown Rd, Apt 1B, Raytown, MO 64133
Amount : \$29,000

Thanks
Sent from my iPhone

Spear Phishing Breakdown

Two major components:

- Sender impersonation
- Call to Action

Sender Impersonation

Approach #1: **CLOSE** email address:

- REAL: seth.nielson@company.com
- FAKE: seth.nielson@c0mpany.com

Approach #2: replace DISPLAY NAME:

- REAL: Seth Nielson <seth.nielson@company.com>
- FAKE: Seth Nielson <seth.nielson@not_even_close.com>

Approach #3: ignore email (get response via link)

Call to Action Psychology

Different than Bulk Phishing

Requires higher success rate

Targets are carefully chosen

Busy people are great targets

Urgency is still stressed

Personal Spear Phishing

urgent ➤

Lei Ding, Ph.D. Security R&D Associate Principal sandrajan92...
to Seth ▼

Seth, Are you free at the moment

Regard

Lei Ding, Ph.D. Security R&D Associate Principal

send from my iPhone.

Spear Phishing Exchange

Okay seth, May when you come down,,i'm so sorry can't place a call right now as I'm tied up at the moment and my network coverage is bad. Please i need a Favor, Can you purchase iTunes gift cards 4 pieces - \$100 each at any nearby store? I would reimburse you when am through later today, Let me know if you can purchase them now with your personal credit card or business card.

regard

Lei Ding, Ph.D. Security R&D Associate Principal

Spear Phishing False Positive?

This message is in response to your request to reset your account's password.

Your username is: sethjn

[Click here to reset your password](#)

If you have not requested a password reset, please [contact Customer Support](#).

If you have any questions, please see the [Help page](#) of the WebStore.

Thank you,

[Johns Hopkins University - Information Security Institute](#)

Whaling

Specifically targets big catches (e.g., CEO)

CEO-like individuals can be vulnerable via assistants

Have a great deal of power that is not questioned

Whaling Techniques

Techniques Used in Whaling

Whaling attacks commonly make use of the same techniques as spear phishing campaigns. Here are a few additional tactics that malicious actors could use:

- **Infiltrate the network:** A compromised executive's account is more effective than a spoofed email account. As noted by **Varonis**, digital attackers could therefore use malware and rootkits to infiltrate their target's network.
- **Follow up with a phone call:** The **United Kingdom's National Cyber Security Centre** (NCSC) learned of several instances where attackers followed up a whaling email with a phone call confirming the email request. This **social engineering** tactic helped to assuage the target's fears that there could be something suspicious afoot.
- **Go after the supply chain:** Additionally, the NCSC has witnessed a rise of instances where malicious actors have used information from targets' suppliers and vendors to make their whaling emails appear like they're coming from trusted partners.

Source:

<https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/>

Real Estate Scams

Closing for 2 15th St NW, Washington, DC 20024



from: **me** <Michelle@lenderusa.com> ✕

Mar 7, 2018, 12:31 PM ⋮

to: John.Homebuyer@gmail.com; Larry@legalaide.com

Hello John,

My name is Michelle and I will be your lender concierge for the closing of your home purchase. I have also copied Larry who will be the attorney assisting me. Look forward to working with you, stay tuned for more information.

Very truly yours,

Michelle
Lender USA, Inc.
Phone: [\(206\) 555-1258](tel:2065551258)

Malicious Email and Psychology

Psychological Manipulation

Similar to Anderson's example about *pretexting*

Emotional impulses drive the reactions

WE ARE ALL VULNERABLE TO THIS

Dealing with Phishing Risk

Don't click on links is best

If you click a link, make sure it is HTTPS

Make sure the URL is correct

Find a phone number via HTTPS website

SLOW DOWN! Send it to an expert for review

Social Media Threats

Includes all the threats from email:

- Spam
- Phishing
- Spear Phishing

Additional Threats

- Attacks on reputation
- Harassment/Bullying
- False information
- False popularity

Social Media Spam/Phishing

Can be used as recon for email-based spear phishing

Spam exists in Facebook, etc

(Spear) Phishing with links for call-to-action

Psychology of Disinformation

People tend to believe popular ideas

This is not necessarily a weakness

None of us can investigate everything

The “wisdom of crowds” is real

NO, YOU CAN'T GO.

BUT ALL MY FRIENDS—
IF ALL YOUR FRIENDS
JUMPED OFF A BRIDGE,
WOULD YOU JUMP TOO?

OH JEEZ. PROBABLY.



WHAT!?! WHY!?!

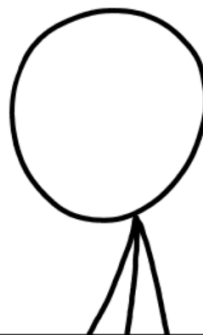
BECAUSE ALL
MY FRIENDS DID.

THINK ABOUT IT—
WHICH SCENARIO
IS MORE LIKELY:



EVERY SINGLE PERSON I KNOW,
MANY OF THEM LEVELHEADED AND
AFRAID OF HEIGHTS, ABRUPTLY WENT
CRAZY AT EXACTLY THE SAME TIME...

...OR THE BRIDGE IS ON FIRE?



...I, UH... HMM.

IMAGINE READING THIS ON CNN: "MANY
FLED THEIR VEHICLES AND JUMPED FROM
THE BRIDGE. THOSE WHO STAYED BEHIND..."

IS SOMETHING GOOD ABOUT
TO HAPPEN TO THOSE PEOPLE?

MAYBE THEY'LL
FIND COOKIES?

OK, YOU STAY.
I'M JUMPING.



Social Media Bots

Bots are automated social media accounts

Simple uses include increasing “friends” count

Can also spread information

Programming is simple: retweet or share

Psychology of Sharing

Bots not always required

Identify something people want to believe

Media consultants test most persuasive formulations

Release into “the wild” and evaluate the spread

Political operatives monitor effectiveness

Political/Social Media Circle

Political machine identifies a target topic

Multiple allied outlets release variable formulations

Track statistics carefully (e.g., Twitter “ratio”)

Anything with backlash can be disavowed easily

Anything that grows popular will be adopted

Politician now publicly adopts position

(Use bots and manipulation too)

Cyberbullying

Simple form

- non-stop harassment
- Unending texts, posts, etc

Other forms

- Release of personal info
- Revenge pornography
- Stealing accounts, passwords
- Spreading false information

Destroying Lives

Nobody is perfect

Some people said things they later regret

People can be socially destroyed for an old tweet

Employers regularly search social media now

Some demand access if your account isn't public

Weak Tech Solutions

The security issues I've raised are hard to solve

Exiting a platform isn't always enough

- Sometimes required for work
- Doesn't stop false posting

Zerofox is a security company that makes an attempt

- Check out "Your Public Attack Surface"

Intrinsic Social Media Threat

There are risks from using social media at all

Network owners incentivized to “always on” usage

Ads and tracking are intrinsic to the (current) model

Inhibit human social development (e.g., empathy)

No More FOMO: Limiting Social Media Decreases Loneliness and Depression

Method: After a week of baseline monitoring, 143 undergraduates at the University of Pennsylvania were randomly assigned to either limit Facebook, Instagram and Snapchat use to 10 minutes, per platform, per day, or to use social media as usual for three weeks.

Results: The limited use group showed significant reductions in loneliness and depression over three weeks compared to the control group. Both groups showed significant decreases in anxiety and fear of missing out over baseline, suggesting a benefit of increased self-monitoring.

Discussion: Our findings strongly suggest that limiting social media use to approximately 30 minutes per day may lead to significant improvement in well-being.

Melissa G. Hunt, Rachel Marx, Courtney Lipson and Jordyn Young

Published Online: December 2018 • <https://doi.org/10.1521/jscp.2018.37.10.751>

Phishing Competition Submission

Updating Direct Deposit



Ellie Daw <Ellie.Daw@crims0nvista.com>

1:16 PM

To: Seth Nielsen <Seth.Nielsen@crimsonvista.com>

Hi Seth,

I recently switched banks and need to update my direct deposit information. My new bank account information is:

Acct #: 9089273541

Routing #: 011401533

Please use this account to deposit my next paycheck. Thanks.

Best,

Ellie Daw
Research Scientist
Crimson Vista
Main: (512) 387-4310
Ellie.Daw@crims0nvista.com
www.CrimsonVista.com