
# HOW HUMAN BEHAVIOR AND DECISION MAKING EXPOSE USERS TO PHISHING ATTACKS

BY INA WANCA AND ASHLEY CANNON

CITIZENS CRIME COMMISSION
OF NEW YORK CITY

# WHY BEHAVIOR MATTERS IN CYBERSECURITY

Cybercriminals use phishing and social engineering to defeat data and system security by exploiting weaknesses in decision making and human behavior.

> Approximately 95% of cyber attacks and events involve preventable human error and behavior weakness.[1]

This number suggests that Internet users are vulnerable, independently of platforms and software. As behavioral scientists have argued, psychology plays an important role in providing answers to why individuals engage in risky cybersecurity practices.[2] Therefore, there are cybersecurity areas and problems where behavioral science could be applied and could have a positive impact on users' cybersecurity habits.

This report asserts that cybersecurity behavior relies on decision making, and, therefore, Internet users must be aware of the ways their behaviors and decision making expose them to cyber-threats.

# WHAT IS PHISHING?

Phishing is a form of fraud where cybercriminals attempt to collect information from a user by posing as a legitimate source (e.g., financial institution) to steal personal information, money, financial data, trade secrets, or gain access to computer systems, among other activities.[3]

In phishing attacks, cybercriminals utilize manipulation and deception to trick users into providing the requested information (i.e., social engineering). Such tactics make it difficult for users to accurately identify fraudulent emails. In fact, only 3% of the more than 19,000 people from around the world that took Intel Security's 2015 Phishing Quiz identified every phishing email correctly; and 80% of quiz takers incorrectly identified at least one phishing email.[4]

Given that it only takes one email to fall victim to a cybercriminal's attack, it is important for users to understand:

- the potential impacts on victims;
- the tactics used in phishing scams; and
- behavior modifications that users can implement to protect themselves and their families, friends, schools and employers.

# HOW PHISHING IMPACTS YOU

Cybercriminals may use phishing scams to steal credentials (e.g., usernames, passwords) and other personal information to gain access to personal or work accounts to steal money, financial or health data, trade secrets, or other sensitive information, or to carry out other crimes, such as identity theft, corporate espionage, or extortion, among other acts.[5]

The information obtained through phishing scams can also lead to further victimization. For example, if a user's personal information (e.g., name, address, telephone number, email account) is posted online, other criminals may use this information to commit other crimes against the victim (e.g., stalking, harassment, burglary).[6]

Victims may even be at risk of becoming suspects in crimes committed by a criminal using their identity or credentials. For example, the cybercriminal may use the victim's credentials to steal money from their employer via an illegal wire transfer.[7]

Moreover, both the personal and professional lives of victims of cybercrimes can be impacted in a wide range of ways, such as:

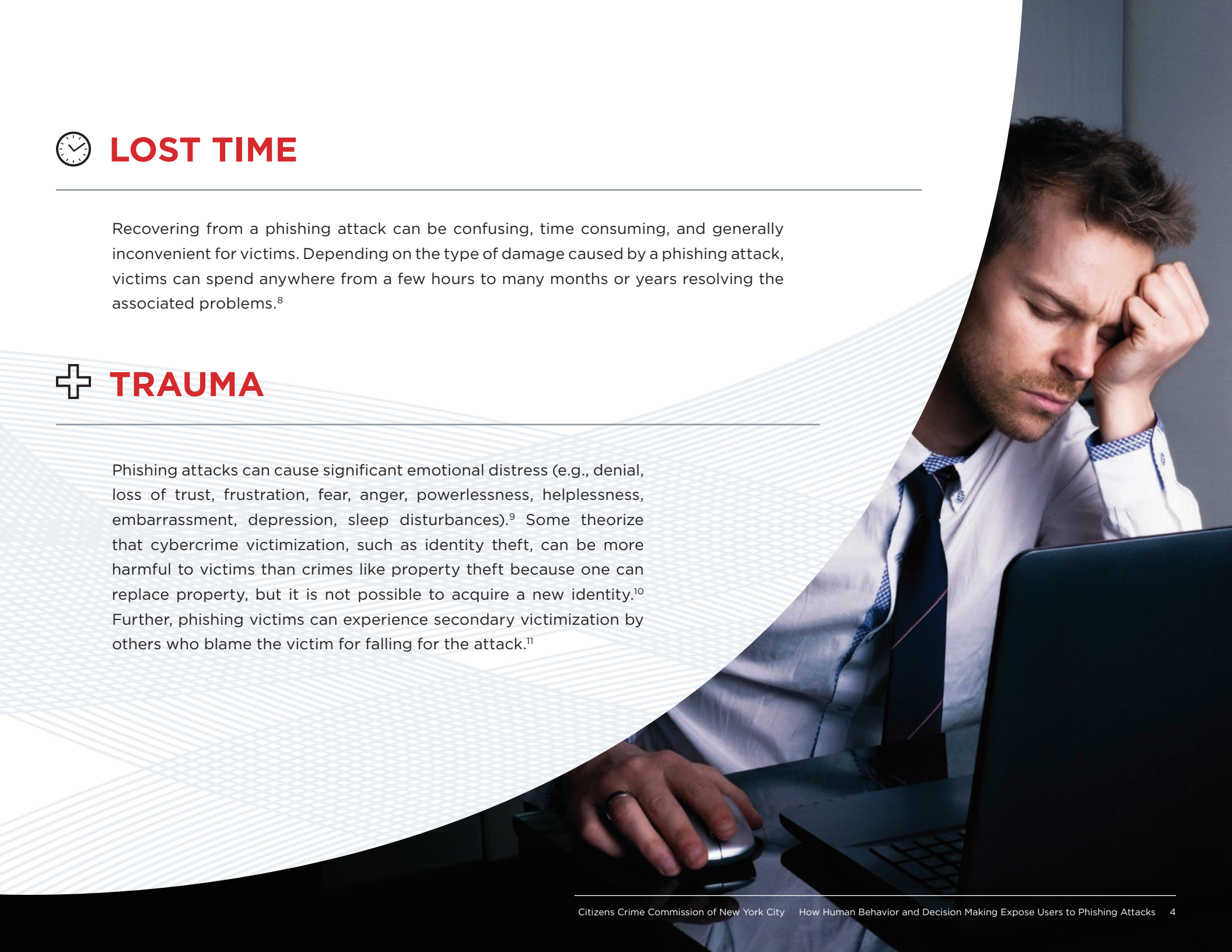
- lost time;
- trauma;
- financial loss;
- social consequences;
- business consequences; and
- lost productivity.

## LOST TIME

Recovering from a phishing attack can be confusing, time consuming, and generally inconvenient for victims. Depending on the type of damage caused by a phishing attack, victims can spend anywhere from a few hours to many months or years resolving the associated problems.[8]

## TRAUMA

Phishing attacks can cause significant emotional distress (e.g., denial, loss of trust, frustration, fear, anger, powerlessness, helplessness, embarrassment, depression, sleep disturbances).[9] Some theorize that cybercrime victimization, such as identity theft, can be more harmful to victims than crimes like property theft because one can replace property, but it is not possible to acquire a new identity.[10] Further, phishing victims can experience secondary victimization by others who blame the victim for falling for the attack.[11]

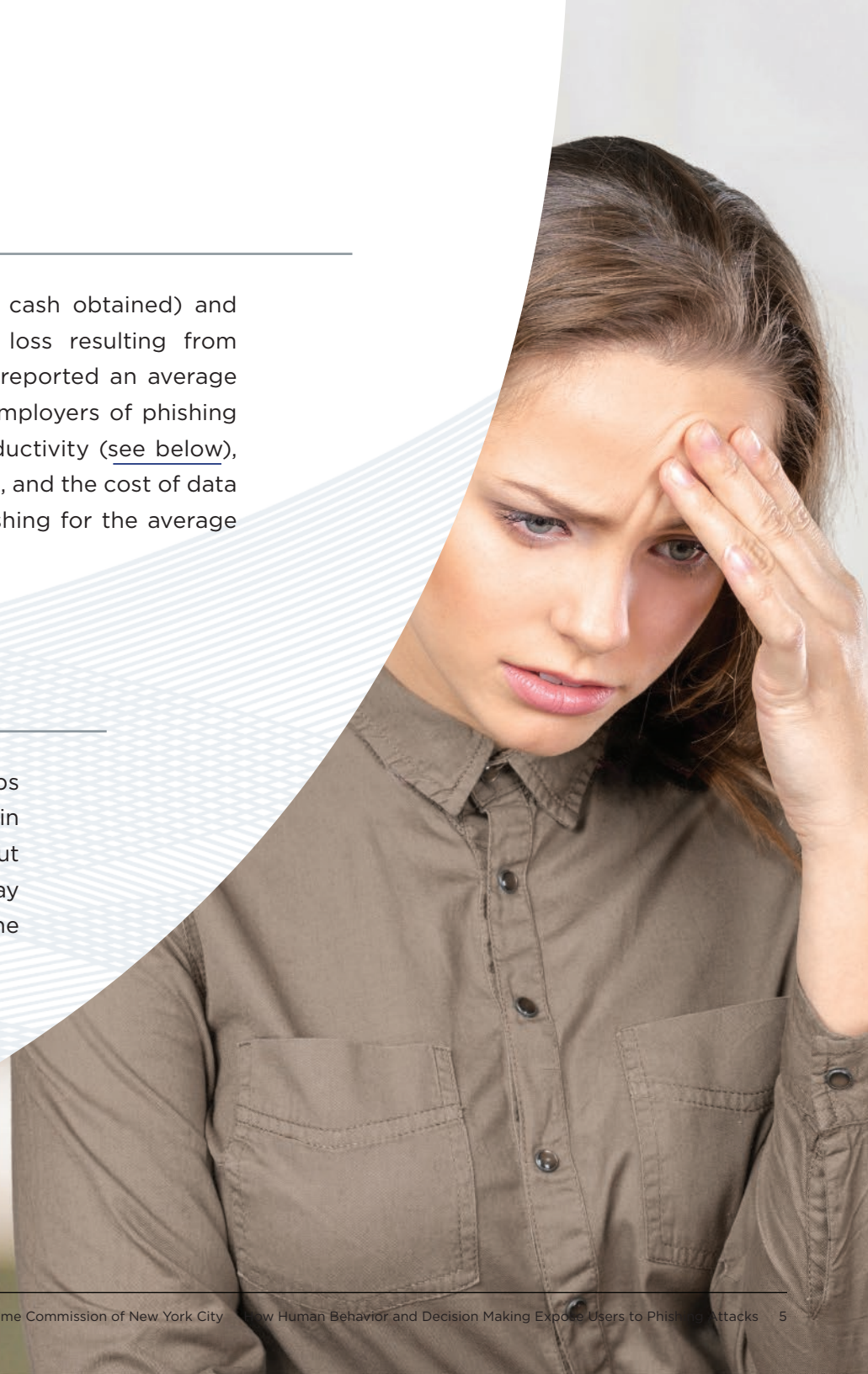


# FINANCIAL LOSS

Victims can incur both direct (i.e., value of goods, services, or cash obtained) and indirect (e.g., legal fees, bounced checks, postage) financial loss resulting from phishing attacks. For example, in 2014, victims of identity theft reported an average combined direct and indirect loss of $1,343.12. In addition, the employers of phishing victims can experience financial losses related to decreased productivity (see below), business disruption, isolating malware and credential compromises, and the cost of data breaches. Researchers estimate that the total annual cost of phishing for the average 10,000-employee company is $3.77 million.[13]

# SOCIAL CONSEQUENCES

Victimization can cause strain on personal and family relationships and reputational damage. For example, if cybercriminals gain access to a victim's email, they can uncover information about personal relationships or embarrassing photos or videos that may be leaked to the public.[14] Family or friends could also become the targets of cybercriminals.



# BUSINESS CONSEQUENCES

Both intellectual property and customer data can be at risk when a phishing attack occurs. In addition to financial loss, a phishing attack can damage the reputation and credibility of a business. Consumers may lose trust in the business, which can lead the company to lose its customer base.[15] Moreover, cyber-espionage typically begins with phishing when employees interact with malicious attachments or follow links to malicious websites. This initial attack allows cybercriminals to gain backdoor access and install malware on computers/devices to further penetrate a system network.[16] Given that it can take months to years to detect a network compromise and it only takes minutes to steal information off a network,[17] cybercriminals can have long periods of undetected access to trade secrets that can hinder business growth.

# LOST PRODUCTIVITY

The time it takes to recover from a phishing attack and the trauma inflicted can result in decreased employee productivity. It is estimated that non-IT employees spend an average of 4.16 hours per year dealing with phishing attacks.[18] The related cost of productivity losses is estimated to be $1.8 million—accounting for 48% of the total organizational costs.[19] Further, productivity can also be lost in preventing phishing attacks, as employees spend time determining if an email is fraudulent.

## INTELLECTUAL PROPERTY

AT RISK FROM PHISHING

**COPYRIGHT**

**PATENT**

**TRADEMARK**

**TRADE SECRETS**

# WHY IS PHISHING A SUCCESSFUL TRICK?

Phishing attacks often rely on a combination of tactics that are known to influence human decision making, such as:

## AUTHORITY

Research has found that people tend to comply with requests from authority figures.[20] Thus, phishing scams claim to be from a trusted source by using a corporate logo or name as the sender to attempt to create legitimacy and credibility.[21]

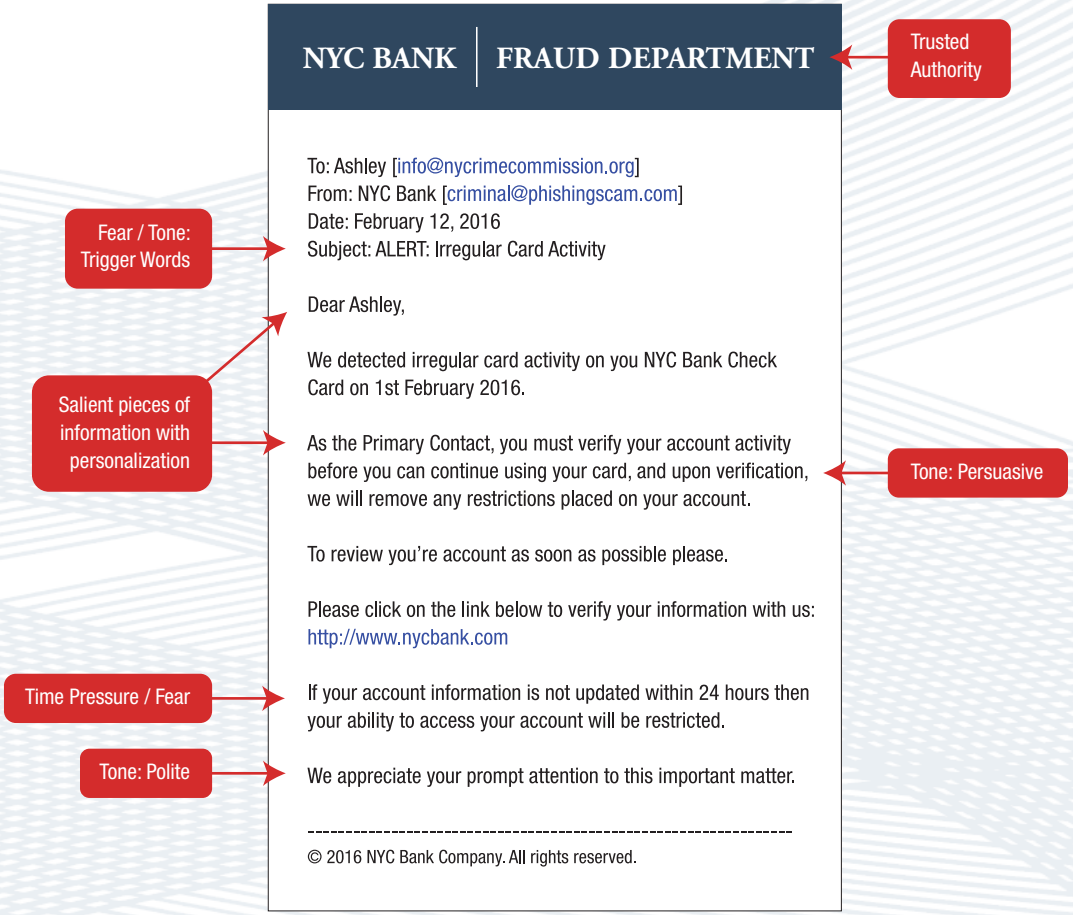
## TIME PRESSURE

Phishing scams may request a rapid response to pressure users to act quickly, and decrease the time users have to uncover the scam.[22]

## TONE

Phishing scams often use a formal tone with a combination of persuasive and polite statements to influence user decision making. Examples include: polite salutations and closures (e.g., Dear, Thank you, Kind regards); trigger words (e.g., alert, warning, attention); and persuasion (e.g., upon verification, restrictions will be removed).[23]

### FIGURE 1: PHISHING TACTICS



# WHY IS PHISHING A SUCCESSFUL TRICK?

## SALIENT PIECES OF INFORMATION

Phishing scams may include a personalized message or salient pieces of information (e.g., primary account contact) to persuade a user that the email is legitimate.[24] In targeted phishing attacks (i.e., spear-phishing), cybercriminals build a target profile based on public information (e.g., employer websites, social media) to craft more authentic appearing messages. By acquiring key insider knowledge (e.g., job functions, work relationships), cybercriminals can increase the likelihood of a successful attack.

## FEAR

Phishing scams may prey on users' fear of something to manipulate them into acting. Cybercriminals may invoke fear by making threats (e.g., account restrictions) or leveraging current events (e.g., natural disasters, health epidemics, economic concerns, political elections, holidays).[25] (*see Case 1*)

### CASE 1:

## CYBERCRIMINALS EXPLOIT FEAR

In 2009, cybercriminals sent emails that appeared to be from the Center for Disease Control and Prevention stating that a state vaccination program was implemented to combat the swine flu and requested that users create a personal vaccination profile by clicking a link that appeared to be the cdc.gov website and enter their personal information.[26]

# PREVENTING PHISHING ATTACKS REQUIRES BEHAVIOR CHANGE

In general, phishing attacks rely on a combination of behavior factors to influence users. Cognitive biases and heuristics can affect how individuals perceive risk and can explain why users exhibit poor cyber habits. For example:

- Users may be overconfident, believing that they will not be the target of a cyber attack (i.e., optimism bias), decreasing the likelihood that a user will seek additional information to determine the legitimacy of the request (e.g., checking the email address, calling the sender);[27] or

- Users may believe that cybersecurity is not an issue relevant to them because they have not been a victim or known a victim recently (i.e., availability heuristic), leading them to delegate cybersecurity measures to others.[28]

Cognitive biases and heuristics can make users more vulnerable to phishing attacks. Therefore, users must incorporate behavior changes into their regular online activities to prevent successful phishing attacks (*see Figure 2*).

# PHISHING PREVENTION TIPS

## 1. CHECK THE SENDER

- Are the name and the email address the same? (e.g., the "from" address text says the institution's name but the email address does not.)
- Does the email address have the same domain name as the company's website? Look out for variations in spelling and domain (.com, .net).
- Unsure? Contact the sender or company directly using information on your account statement or found online. Do not use the email address, phone, or website included in the message.

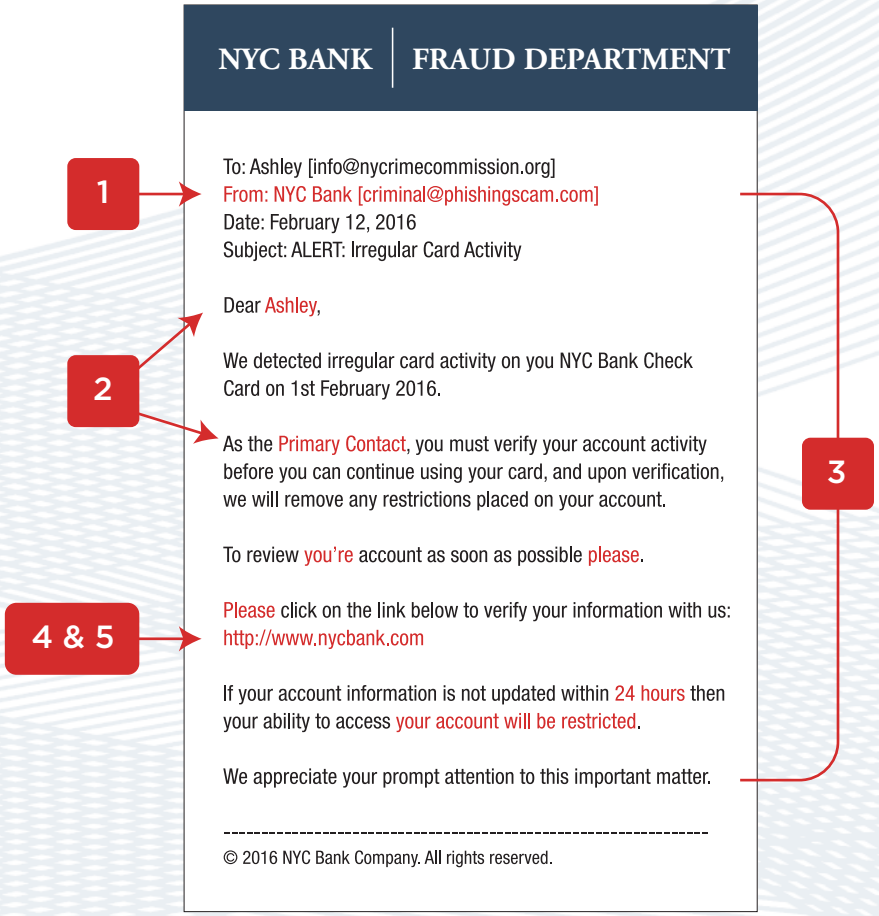
## 2. IDENTIFY RECIPIENT OF THE EMAIL

- Does the salutation include your name?
- If it includes salient pieces of information, are those accurate? (e.g., are you the primary contact on the account?)

## 3. CAREFULLY READ THE MESSAGE

- Does the message contain errors such as typos and poor grammar?
- Does the message contain threats or invoke fear?
- Does the message request an urgent action?

### FIGURE 2: BEHAVIOR MODIFICATIONS



# PHISHING PREVENTION TIPS

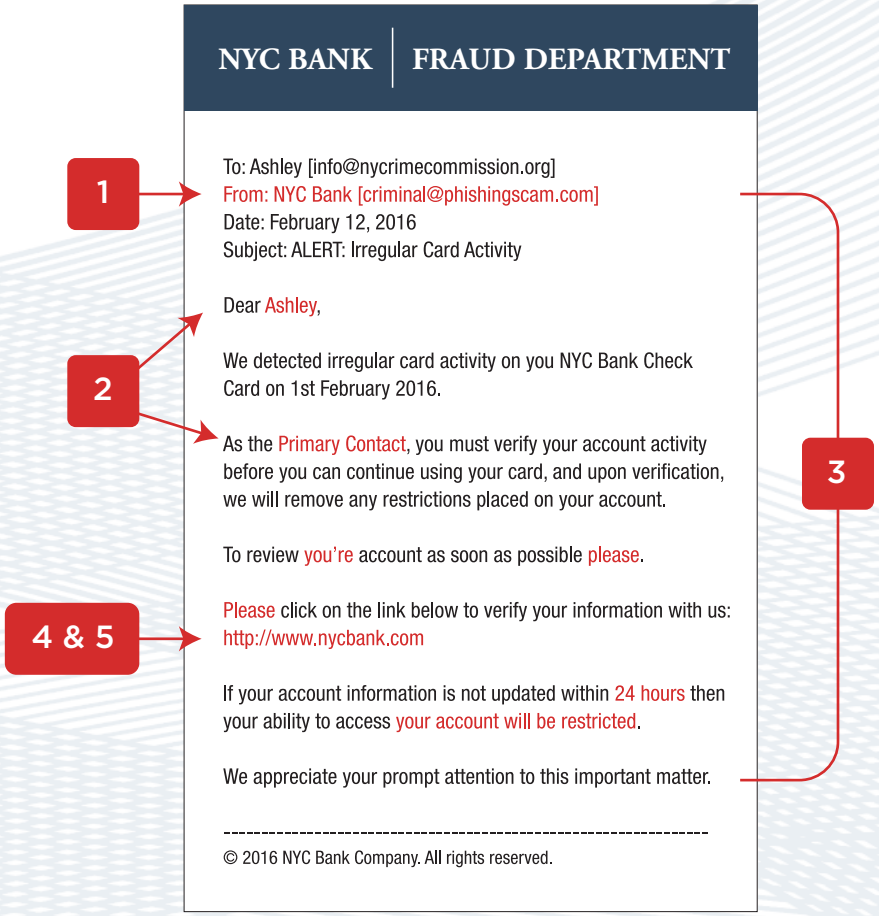
## 4. KNOW WHERE LINKS WILL TAKE YOU

- Check the URL before clicking any link (hover over the hyperlink with the mouse pointer)
    - Do the hyperlinked text and the URL match?
    - Is the domain in the URL the same as the company's website?
- Look out for variations in spelling and domain (.com, .net).
- Type the website address into the browser instead of clicking the link.

## 5. THINK BEFORE YOU CLICK LINKS, OPEN ATTACHMENTS, OR DOWNLOAD SOFTWARE

- Don't open attachments or click links that you are not expecting.
- Ensure your anti-virus software/security settings are up-to-date and enabled before opening an attachment, downloading or clicking a link.

### FIGURE 2: BEHAVIOR MODIFICATIONS



# FINALLY, IF YOU THINK YOU HAVE BEEN A VICTIM OF CYBERCRIME:

- ✓ CHANGE YOUR PASSWORDS IMMEDIATELY
- ✓ CONTACT THE REAL INSTITUTION WHERE YOU HAVE THE ACCOUNT
- ✓ REPORT THE INCIDENT TO IC3.GOV AND TO YOUR EMPLOYER
- ✓ CREATE AND IMPLEMENT AN IDENTITY THEFT RECOVERY PLAN BY VISITING IDENTITYTHEFT.GOV

# ENDNOTES


1. IBM Global Technology Service, Managed Security Services, *IBM Security Services 2014 Cyber Security Intelligence Index* (2014 June) http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/index.html
2. B.K. Wiederhold, "The Role of Psychology in Enhancing Cybersecurity," *Cyberpsychology, Behavior, and Social Networking 17*(3) (2014): 131-32.
3. G. Aaron, *Phishing Trends Report 1st – 3rd Quarters 2015* (Anti-Phishing Working Group (APWG), 2015) http://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf ; Microsoft, "Phishing: Frequently Asked Questions," Safety & Security Center https://www.microsoft.com/en-us/security/online-privacy/phishing-faq.aspx
4. G. Davis, "Here's How the World Fared on Our Phishing Attack Quiz," *McAffe Blog* (2015 May 12) https://blogs.mcafee.com/consumer/phishing-quiz-results/
5. MH. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, 2nd Edition (Burlington, MA: Jones & Bartlett Learning, 2014).
6. G. Kirwan & A. Power, *The Psychology of Cyber Crime: Concepts and Principles* (Hershey, PA: Information Science Reference, 2012).
7. S. Hoffman, "China Source of Illegal Wire Transfers, FBI Warns," *CRN* (2011 April 27) http://www.crn.com/news/security/229402349/china-source-of-illegal-wire-transfers-fbi-warns.htm ; A. Valenti & S. Korinko, *Fake Domain Wire Transfer Scheme: How to Recognize the Fraud and Protect Your Company* (New York: Stroz Friedberg, 2014) http://www.strozfriedberg.com/wp-content/uploads/2014/10/SF_FakeDomainWireTransferScheme_102020147PM.pdf
8. E. Harrell, "Victims of Identity Theft, 2014," *Bulletin* (NCJ 248991) (Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2015 September) http://www.bjs.gov/content/pub/pdf/vit14.pdf ; Synovate, *Federal Trade Commission – 2006 Identity Survey Report* (2007 November) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf
9. Identity Theft Resource Center, *Identity Theft: The Aftermath 2014* (2015) http://www.idtheftcenter.org/images/surveys_studies/Aftermath2014FINAL.pdf ; Symantec Corporation, *Norton Cybercrime Report: The Human Impact* (2010) http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf
10. C. Ess, *Digital Media Ethics* (Cambridge, England: Polity Press, 2009).
11. G. Kirwan & A. Power, *The Psychology of Cyber Crime: Concepts and Principles* (Hershey, PA: Information Science Reference, 2011).
12. E. Harrell, "Victims of Identity Theft, 2014," *Bulletin* (NCJ 248991) (Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2015 September) http://www.bjs.gov/content/pub/pdf/vit14.pdf
13. Ponemon Institute LLC, *The Cost of Phishing & Value of Employee Training* (2015 August) http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf
14. E. Augenbraun, "Apple Users Targeted in 'Phishing' Scams," *CBS News* (2014 October 02) http://www.cbsnews.com/news/apple-users-targeted-in-phishing-scams/
15. America Association for the Advancement of Science, "DOE Laboratories in the Spotlight," *Science 213*(4509) (1981): 744; PwC, *Cybercrime in the Spotlight Swiss Economic Crime Survey 2011* (2011 November) https://www.pwc.ch/user_content/editor/files/publ_adv/pwc_global_economic_crime_survey_11_CH_e.pdf
16. Verizon, *2015 Data Breach Investigations Report: Intellectual Property Theft* (2015) http://www.verizonenterprise.com/resources/reports/rp_dbir-intellectual-property-theft-2015_en_xg.pdf
17. Mandiant, *M-Trends 2015: A View from the Front Lines* (2015) https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
18. Ponemon Institute LLC, *The Cost of Phishing & Value of Employee Training* (2015 August) http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf
19. Ponemon Institute LLC, *The Cost of Phishing & Value of Employee Training* (2015 August) http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf
20. R. Cialdini, *Influence: Science and Practice*, 5th Edition (Boston, MA: Pearson Education, 2009).
21. B. Atkins & W. Huang, "A Study of Social Engineering in Online Frauds," *Open Journal of Social Sciences 1*(3) (2013): 23-32 http://file.scirp.org/Html/36435.html
22. B. Atkins & W. Huang, "A Study of Social Engineering in Online Frauds," *Open Journal of Social Sciences 1*(3) (2013): 23-32 http://file.scirp.org/Html/36435.html
23. B. Atkins & W. Huang, "A Study of Social Engineering in Online Frauds," *Open Journal of Social Sciences 1*(3) (2013): 23-32 http://file.scirp.org/Html/36435.html
24. G. Kirwan & A. Power, *The Psychology of Cyber Crime: Concepts and Principles* (Hershey, PA: Information Science Reference, 2011).
25. U.S. Computer Emergency Readiness Team, "Avoiding Social Engineering and Phishing Attacks," *Security Tip* (ST04-014) (2013 February 06) https://www.us-cert.gov/ncas/tips/ST04-014
26. Illinois Department of Public Health, "State Public Health Director Warns Public of H1N1 Phishing E-Mail Scam," *Press Release* (2009 December 03) http://www.idph.state.il.us/public/press09/12.3.09H1N1_EmailPhishingScam.htm
27. G. Kirwan & A. Power, *The Psychology of Cyber Crime: Concepts and Principles* (Hershey, PA: Information Science Reference, 2011).
28. K. Quigley, C. Burns, & K. Stallard, "'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection," *Government Information Quarterly 32*(2) (2015): 108-17.

# HOW HUMAN BEHAVIOR AND DECISION MAKING EXPOSE USERS TO PHISHING ATTACKS


## ACKNOWLEDGEMENTS

This report was prepared by Ina Wanca and Ashley Cannon.
Layout and design by Peter Green.





This report was supported by the Howard and Abby Milstein Foundation.


For more information about the Crime Commission's Cybercrime Prevention initiatives visit our website:
www.nycrimecommission.org

THE CITIZENS CRIME COMMISSION OF NEW YORK CITY IS A NON-PARTISAN NON-PROFIT ORGANIZATION WORKING TO MAKE CRIMINAL JUSTICE AND PUBLIC SAFETY POLICIES AND PRACTICES MORE EFFECTIVE THROUGH INNOVATION, RESEARCH, AND EDUCATION.

CITIZENS CRIME COMMISSION
OF NEW YORK CITY