



Psychology of the Hack

Steve Andrews – Technology Supervisor
Southwest Kansas Library System



**CYBERSECURITY
AWARENESS
MONTH**

October is cybersecurity awareness month.



A hacker at work...

https://commons.wikimedia.org/wiki/File:Wallpapersden.com_anonymous-hacker-working_1280x720.jpg

- What preconceptions do we have about the individual in this image? Sex, age, ethnicity?
Social skills: awkward?
- People utilize preconceptions to help expedite information processing.
- Preconceptions are cognitive biases.
- Preconceived notions of someone or something, based on information we have, perceive to have, or lack.
- Representativeness heuristic




Born: 1963, Van Nuys, Los Angeles, CA

Died: July 16, 2023, Las Vegas, NV

Kevin Mitnick, World's Most Famous Hacker

https://commons.wikimedia.org/wiki/File:Kevin_Mitnick_ex_hacker_y_ahora_famoso_consultor_en_redes_en_Campus_Party_M%C3%A9xico_2010.jpg

- Outward appearances. Sharply dressed, suit & tie, lanyard around neck, in front of microphone. Expert in his field, author.
- Based on the context of this presentation, he has something to do with cybersecurity, or psychology, or perhaps both.
- Is he a “good guy” or a “bad guy”?



Targeted / Hacked Companies, Organizations, Agencies

- Pacific Telephone
- General Telephone
- LAPD
- California DMV
- Los Angeles County Sheriff's Dept
- Digital Equipment Corporation (DEC)
- Sun Microsystems
- Nokia
- Motorola Corporation
- ARPANET
- Pentagon

Kevin Mitnick's career as a hacker is legendary. He had managed to hack many of the companies and organizations in this list before the age of 18.



U.S. Department of Justice
United States Marshals Service

WANTED BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, initiate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (9907_0221460221).

NAME:MITNICK, KEVIN DAVID

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



DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:TAM BUYS, CALIFORNIA
Date(s) of Birth:08/06/63; 10/18/70
Height:5'11"
Weight:190
Eyes:BLUE
Hair:BROWN
Shirt:LIGHT
Scars, Marks, Tattoos:NONE KNOWN
Social Security Number (if):550-39-5695
NCIC Fingerprint Classification:DPM2OPM13D1PM19PM9

ADDRESS AND LOCAL: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED

WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-554-2455).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.

Telephone (800)336-6102 (24 hour telephone contact) NLETS access code is VALDSMOOOO.

PRISON EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form 101a-112
(Rev. 3/79)

November 1992

- In 1992 a federal warrant issued for his arrest.
- He was a fugitive for 2.5 years
- Arrested Feb 1995
- Served five years in prison—four-and-a-half years' pre-trial and eight months in [solitary confinement](#), because, according to Mitnick, law enforcement officials convinced a judge that he had the ability to "start a nuclear war by whistling into a pay phone"
- Released Jan 2000.
- During his supervised release, which ended on January 21, 2003, he was initially forbidden to use any communications technology other than a landline telephone
- Mitnick Security Consulting LLC, a computer security consultancy
- Was part owner of KnowBe4, provider of an integrated platform for security awareness training

What Made Kevin a Talented Hacker?

- The question of what made Kevin so good at hacking lies at the core of this presentation.
- He had technical prowess, and an inquisitive mind.
- However, one skill that Kevin developed above all others made him so good at hacking: social engineering.



Social Engineering

- In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information.
- All social engineering techniques are based on attributes of human decision-making known as **cognitive biases**.
- Kevin Mitnick, like many famous / infamous hackers and criminals, was a master at social engineering.
- Social Engineering can overcome many technical and physical security systems
 - Identity and Access Management
 - Physical Entry Security
 - Internal Confidential Information Access



*“Only amateurs attack machines;
professionals target people.”*

Bruce Schneier

- Bruce Schneier, a widely respected computer security professional, privacy specialist, and writer, made this remark in 2000 in an article concerning the following...
- On 25 August 2000, the press release distribution service Internet Wire received a forged e-mail that appeared to come from Emulex Corp. and said that the CEO had resigned and the company's earnings would be restated.
- Internet Wire posted the press release, not bothering to verify either its origin or contents.
- Several financial news services and Web sites further distributed the false information, and the stock dropped 61% (from \$113 to \$43) before the hoax was exposed.
- \$2.54 billion in market capitalization disappeared (only to reappear hours later as the hoax was uncovered).

Cognitive Bias

Systematic errors in the way individuals reason about the world due to subjective perception of reality.

- Information we have
- Information we perceive to have
- Information we lack

<https://www.britannica.com/science/cognitive-bias>

We've most likely heard of this term, but what does it really mean?

Cyberpsychology



- Looking at cybersecurity through the lens of psychology.
- Inter-disciplinary domain
- Human interaction with digital technology, particularly the Internet
- Not new, but definitely gaining momentum in government and private sector.



Dual Process Theories of Cognition

- Presenter's note on theories
- Daniel Kahneman (psychologist)
- Two parallel systems of thought that perform different functions
 - System 1 is the unconscious, automated cognition
 - Heuristics
 - Fast
 - Evolutionarily old
 - Prior knowledge and beliefs
 - Associative memory
 - Unconscious reasoning
 - System 2 is the conscious, deliberate thinking
 - Slower than system 1
 - Evolutionarily recent
 - Rule based, analytic
 - Finite resource
 - Both System 1 and System 2 processing can lead to normative answers and both can involve cognitive biases.

Proponents and opponents. Theories are systems of ideas meant to explain something or predict phenomena. Example: classical Newtonian Mechanics which works well at the macroscopic level but has given way to quantum mechanics to explain and predict at the sub-atomic level. Dual process cognition in this presentation is used to provide a framework for understanding biases and how they are potentially leveraged against us.

As Dr. Kahneman notes, the idea of these two systems (1 & 2) are akin to homunculi. There exists no physical system 1 and 2 within the human brain.

- System 2 can endorse system 1.
- System 2 resource exhaustion.
- 35,000 decisions a day

Although cognitive biases can lead to irrational decisions, they are generally thought to be a result of mental shortcuts, or **heuristics**, that often convey an evolutionary benefit.



- They are often studied in psychology, sociology and behavioral economics. Cognitive biases are exploited by vendors, marketing, and other entities you may interact with regularly.



System 1 and 2 Notes

- System 1 produces the beliefs for system 2
- System 2 is lazy
- Law of least effort: people do whatever is minimal effort
- 2 needs constant attention and focus to work
- Focusing attention can make people blind
- We are also blind to our blindness
- 2 turns on when 1 is surprised
- 1 has biases
- 1 cannot be turned off
- 2 is in charge of self control
- Cannot prevent system 1 from falling for illusion even if u know different (Müller-Lyer)
- Cognitive illusions also (Monty Hall problem)
- Easier to see mistakes in others than yourself
- System 1 and 2 fictitious concepts

- The selective attention task video, Christopher Chabris and Daniel Simons
- The Müller-Lyer illusion is an optical illusion where two lines of the same length appear to be of different lengths.

Müller-Lyer illusion



Fig. 1.



Fig. 2.

Müller-Lyer illusion - Franz Bretano - 1892



Optimism Bias

People tend to overestimate the probability of positive events and underestimate the probability of negative events happening to them

- illusion of invulnerability



Optimism Bias in Action

- I have (or my organization) has nothing that a hacker would be interested in.
- My password is good enough even though it is simple
- I don't need to use 2FA or MFA because I have a password
- Our organization's cybersecurity can protect us against anything
- Equifax Data Breach - 2017

Availability Bias

- immediate examples that come to a person's mind when evaluating a specific topic, concept, method, or decision.



Availability Bias in Action

- Works by prioritizing infrequent events based on recency and vividness.
- It's all over the news!
- Everyone has been talking about XYZ getting hacked by China

Affect Bias

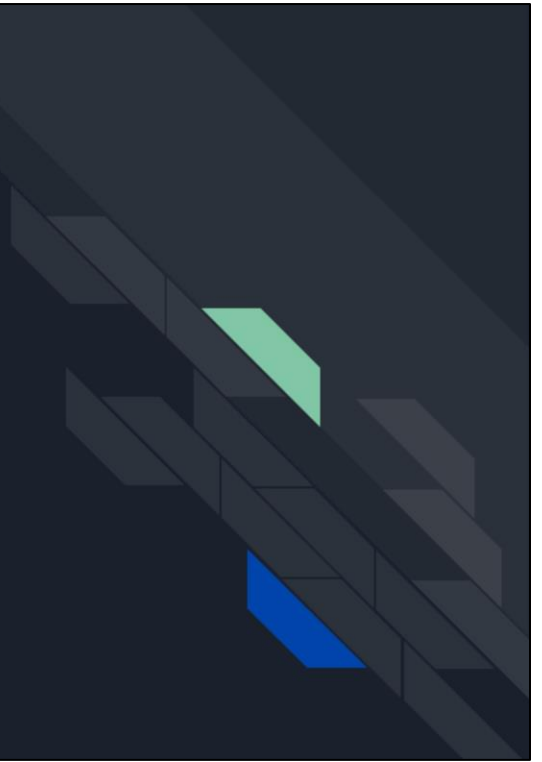
- Instead of evaluating the situation objectively, we rely on our “gut feelings” and respond according to how we feel. As a result, the affect heuristic can lead to suboptimal decision-making.

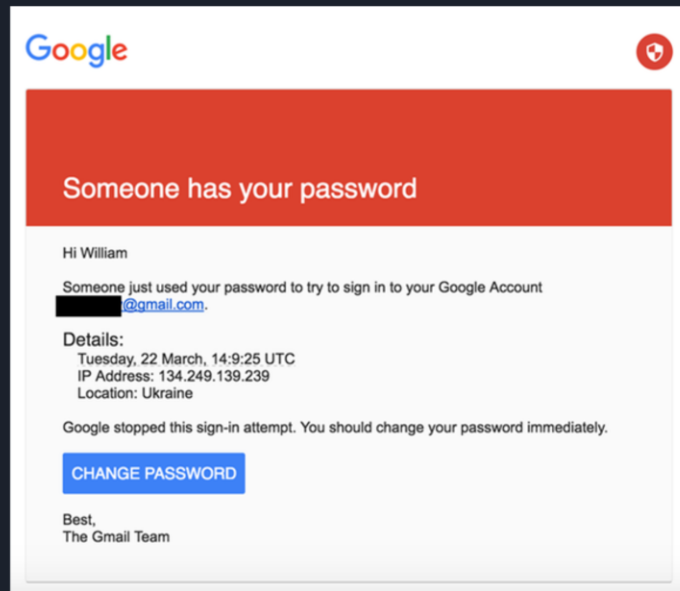


Affect Bias in Action

- Causes us to consult our emotions and feelings when we need to form a judgment but lack the information or time to reflect more deeply.
- My gut says this email is / isn't legitimate
- I like the guy that came and worked on our security camera system, he seemed nice. I hadn't seen him before today though.
- I'm having a really bad day and now my bank emailed me to say my account has been hacked.

Fancy Bear (APT28) and the Clinton Campaign in 2016 - Spear Phishing





Email received by Billy Rinehart March 22, 2016

Hillary Clinton's campaign chairman John Podesta receives a phishing email masked as an alert from Google that another user had tried to access his account. It contains a link to a page where Podesta can change his password. He shares the email with a staffer from the campaign's help desk. The staffer replies with a typo - instead of typing "This is an illegitimate email," the staffer types "This is a legitimate email." Podesta follows the instructions and types a new password, allowing hackers to access his emails.

- [Bad actors from Russia sent a series of spear phishing emails](#) to various individuals in The Democratic National Convention's network, posing as Google warning recipients of suspicious activity on their Google accounts.
- The social engineering email shortened the link using a Bitly URL, hiding its true redirect path.
- Once the shortened link was clicked, the webpage asked recipients to change their password.
- After targets clicked the spoofed link and entered their credentials, the cyber criminals gained full access to their Google account, including their Gmail access, which allowed them to scrub thousands of emails with sensitive information pertaining to the Democratic candidate Hilary Clinton's campaign.



Sign-in attempt was blocked

██████████@gmail.com

Someone just used your password to try to sign in to your account. Google blocked them, but you should check what happened.

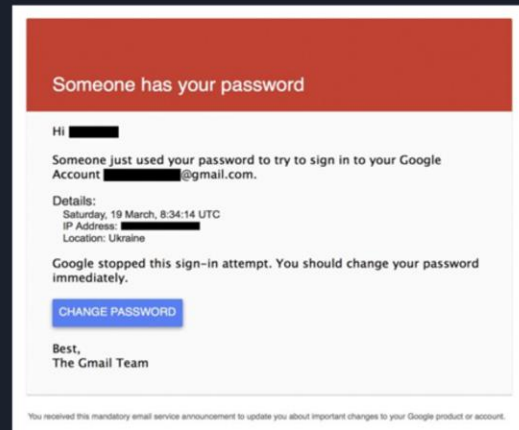
[CHECK ACTIVITY](#)

Actual Google message for blocked sign-in attempt

Fake Email Examination

- Fear – Account has been compromised
- Urgency - pressure to act immediately
- Representativeness - Made to look like the real Google alert
- Availability - Ukraine had been in the news recently
- Affect - High benefit / low risk to click link to reset password
- URL Shortener to fake webpage to reset password
- HTTP rather than HTTPS on password reset webpage

Account(s) did not have 2FA / MFA enabled.



- Representativeness heuristic involves estimating the likelihood of an event by comparing it to an existing prototype that already exists in our minds.
- Availability heuristic describes our tendency to use information that comes to mind quickly and easily when making decisions about the future.
- Affect heuristic: make decisions based on emotion by substituting easier question "what do I feel" for harder question "what do I think"

Heuristics, Shortcuts, and Persuasion





Robert B. Cialdini - 6 Principles of Persuasion

1. Reciprocity: we don't like to feel that we owe other people.
2. Scarcity: The less of something there is, the more people tend to want it. (McRib)
3. Authority: Individuals who are authoritative, credible and knowledgeable experts in their fields are more influential and persuasive than those who are not.
4. Commitment and consistency: if I can convince you to act in a minor way in relation to something, then you'll think of yourself as that type of person and be more likely to act in that way again in the future.
5. Liking: people are much more likely to be influenced and persuaded by those that they like.
6. Consensus (social proof): Humans are social by nature and generally feel that it's important to conform to the norms of a social group.

- “weapons of influence” in the context of sales and marketing, but they are equally applicable to a security context
- Reciprocity: attacker sends email with coupon in exchange for signing up for an account
- Scarcity: McRib! Email that account will be deactivated in x days and link to resolve.
- Authority: Yellow or Orange vest, hardhat, and clipboard.
- Consensus: when there is a natural disaster, there are often several illegitimate organizations posing as a charity to elicit donations.



Common Social Engineering Methods

- Posing as someone in authority
- Pretexting: Masquerading as someone else
- Posing as a vendor or system manufacturer calling to offer unsolicited support
- Offering a prize for registering to a website
- Enticing the victim with promises of something of value
- Threatening to reveal something that the target wishes to be kept secret (blackmail)
- Promising something to the victim in exchange for their help (quid pro quo)
- Mentioning that another employee had helped them in the past



Stanley Rifkin - 1978
Security National Pacific Bank Los Angeles
\$10.2 million

- Working for a company under contract to develop a backup system for the Security Pacific National Bank wire room.
- Rifkin learned of the transfer procedures used, and found that bank agents would frequently write down the daily transfer code.
- One day in mid-October 1978, he made his way into the transfer room, saw the code, memorized it and walked out.
- He then made a few phone calls and had \$10.2 million wired to the Irving Trust Company in New York City for the credit of the Wozchod Handels Bank of Zurich in Switzerland, where he'd already set up an account.

- The Lufthansa heist which took place at New York City's John F. Kennedy International Airport on December 11, 1978 netted an estimated US\$ 5.875 million
- Of the two robberies, the Lufthansa heist received more media coverage
- Media affects the Availability heuristic (immediate / recent events that come to mind when making a decision)



Gragg's (2003) Seven Psychological Triggers

1. Strong affect. A person in a heightened emotional state (e.g. fearful, excited) is less likely to think reasonably and more likely to be influenced or persuaded.
2. Overloading. When a person is rapidly given too much information, their senses are overloaded, and they are unable to logically evaluate the given arguments.
3. Reciprocation. People tend to follow the social rule of "returning the favor," repaying social debts to others who (appear to) have helped them in the past.
4. Deceptive relationships. An attacker who establishes a relationship with a victim under false pretenses (e.g. giving the victim information, mentioning a common enemy) can build trust and more easily exploit their victim.
5. Diffusion of responsibility and moral duty. People can be manipulated into feeling that they will not be held solely responsible for their actions, or that their actions are their "moral duty".
6. Authority. People are conditioned to respond to, and not to question, someone who is supposedly in authority.
7. Integrity and consistency. People tend to follow through with what they say they will do and usually believe that others are honest and truthful.



Warning Signs

- Stressing urgency or negative consequences of noncompliance
- Inundate with information (effect similar to choice overload)
- Offer of free goods or services, unsolicited offer of help
- Name dropping, unsolicited information
- Decision for success or failure of another employee where you will not be held responsible (moral duty) -> help me or I may be fired
- Unknown person with alleged / professed authority or knowledge
- Pressured to fulfil commitment made by you or another person (guard your vacation calendars!)




Cyber Hacks that Utilize Components of Social Engineering

- Scareware (pop-ups, email)
- Phishing emails and snail mail
 - Unrecognized invoice
 - Undeliverable packages (FedEx, UPS, etc.)
 - Problem with an account
 - Payment or remittance for unknown goods or services
 - Confirm personal or financial information
 - Looks similar to a legit service - Annual Website Domain Listing !!!
- Spear Phishing (targeting people specifically or with more recon beforehand)
- Vishing (voice phishing)
 - Posing as an employee of a legitimate body such as the bank, telephone or internet provider
 - Pose as law enforcement or as an Internal Revenue Service employee
 - Often target immigrants and the elderly



Why Phishing, Spear Phishing, and Vishing Succeed

- Authority
- Strong Affect (time / pressure / urgency)
- Halo Effect (positive impression of company or brand)
- Reciprocity
- Scarcity
- Integrity or Moral Obligation (pay company or personal bills)
- Representativeness (comparing similarity)
- Availability (immediate / recent events that come to mind when making a decision)

- 
- A joint study by Stanford University Professor Jeff Hancock and security firm Tessian has found that **88%** of data breach incidents are caused by employee mistakes.

- Similar research by IBM Security puts the number at 95%.

People are generally
bad at statistics.



An individual has been described by a neighbor as follows:

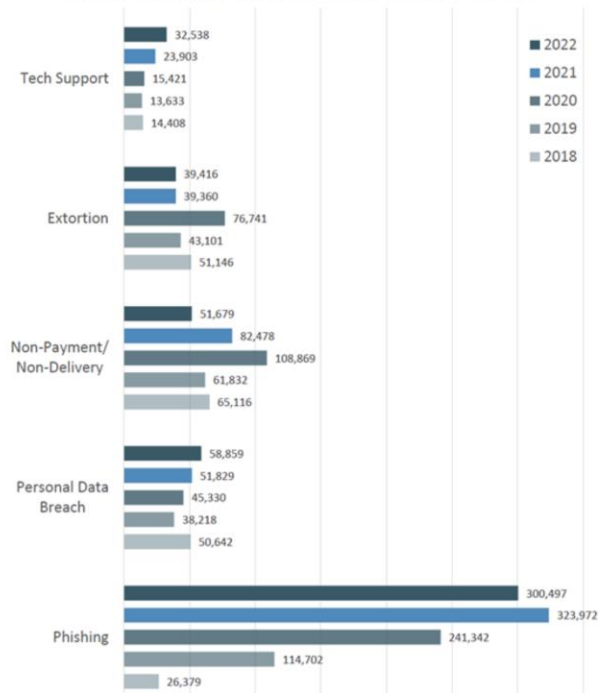
“Steve is very shy and withdrawn, invariably helpful but with little interest in people or in the world of reality. A meek and tidy soul, he has a need for order and structure, and a passion for detail.”

Daniel Kahneman, Thinking, Fast and Slow

Availability bias and stereotyping. Associative memory. The resemblance of Steve's personality to that of a stereotypical librarian. Male farmers in the United States outnumber male librarians by a ratio of about 20 to 1.

Bayes formula, based on approx. 166,000 librarians (ALA fact sheet 2012), 2.6 million farmers (USDA 2021), the description fitting 70% of librarians and 30% of farmers would yield the likelihood that Steve is a librarian at approx. 14%

Top Five Crime Types Compared with the Previous Five Years



- Internet Crime Complaint Center (IC3) 2022 Report

CALL CENTER FRAUD¹²



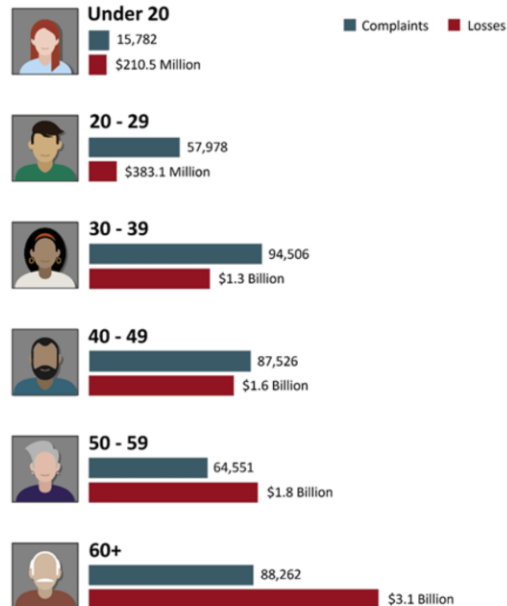
TECH AND CUSTOMER SUPPORT/GOVERNMENT IMPERSONATION

Illegal call centers defraud thousands of victims each year. Two categories of fraud reported to the IC3, Tech/Customer Support and Government Impersonation, are responsible for over \$1 billion in losses to victims.

| | Victims | Losses | Trend |
|---------------------------|---------------|------------------------|--------|
| Government Impersonation | 11,554 | \$240,553,091 | ▲ 68% |
| Tech and Customer Support | 32,538 | \$806,551,993 | ▲ 132% |
| TOTAL | 44,092 | \$1,047,105,083 | |

- Call centers overwhelmingly target the elderly, with devastating effects. Almost half the victims report to be over 60 (46%), and experience 69% of the losses (over \$724 million).
- Internet Crime Complaint Center (IC3) 2022 Report

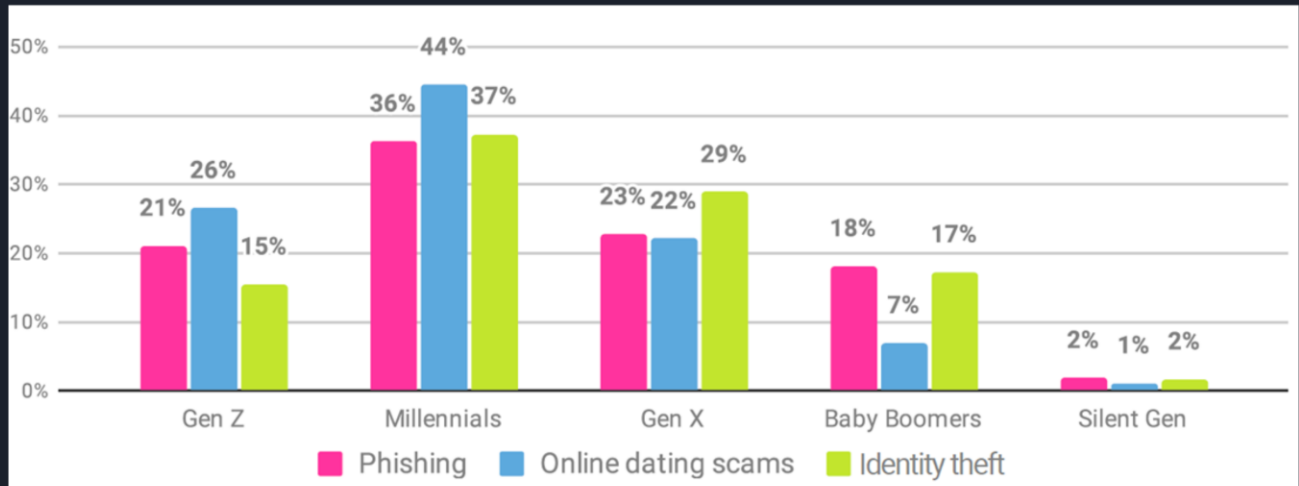
2022 - VICTIMS BY AGE GROUP¹⁷



- Not all complaints include an associated age range—those without this information are excluded from this table.
- Internet Crime Complaint Center (IC3) 2022 Report

| By Victim Count | | | |
|--------------------------|---------|---------------------------------|---------|
| Crime Type | Victims | Crime Type | Victims |
| Phishing | 300,497 | Government Impersonation | 11,554 |
| Personal Data Breach | 58,859 | Advanced Fee | 11,264 |
| Non-Payment/Non-Delivery | 51,679 | Other | 9,966 |
| Extortion | 39,416 | Overpayment | 6,183 |
| Tech Support | 32,538 | Lottery/Sweepstakes/Inheritance | 5,650 |
| Investment | 30,529 | Data Breach | 2,795 |
| Identity Theft | 27,922 | Crimes Against Children | 2,587 |
| Credit Card/Check Fraud | 22,985 | Ransomware | 2,385 |
| BEC | 21,832 | Threats of Violence | 2,224 |
| Spoofing | 20,649 | IPR/Copyright/Counterfeit | 2,183 |
| Confidence/Romance | 19,021 | SIM Swap | 2,026 |
| Employment | 14,946 | Malware | 762 |
| Harassment/Stalking | 11,779 | Botnet | 568 |
| Real Estate | 11,727 | | |

- Internet Crime Complaint Center (IC3) 2022 Report



•

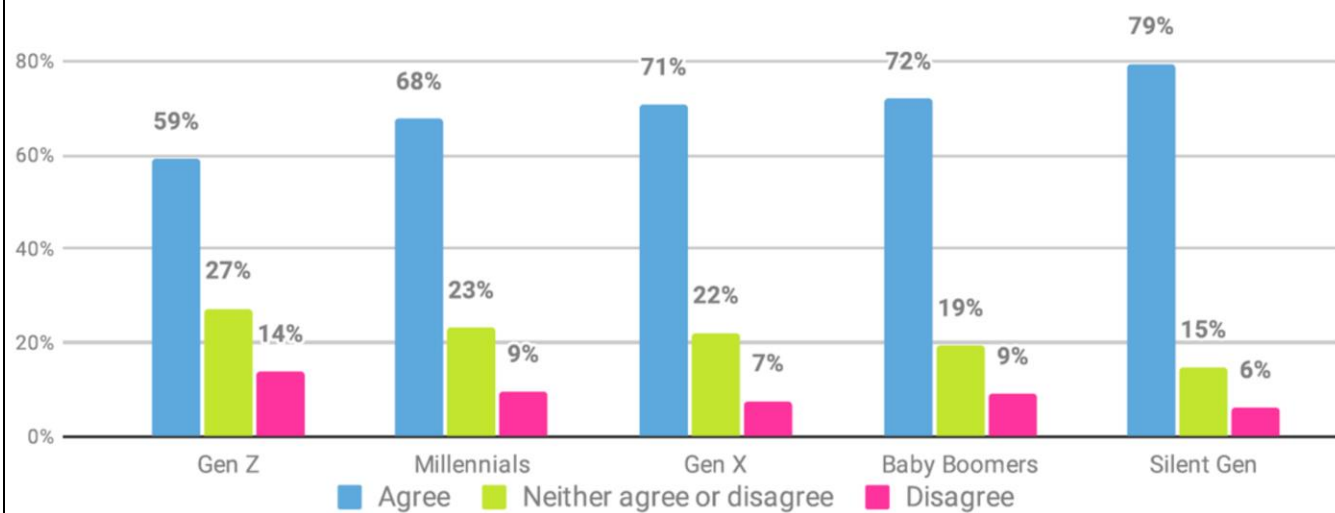


Figure 34. Participants' levels of agreement when answering "I feel that staying secure online is achievable" by generation.

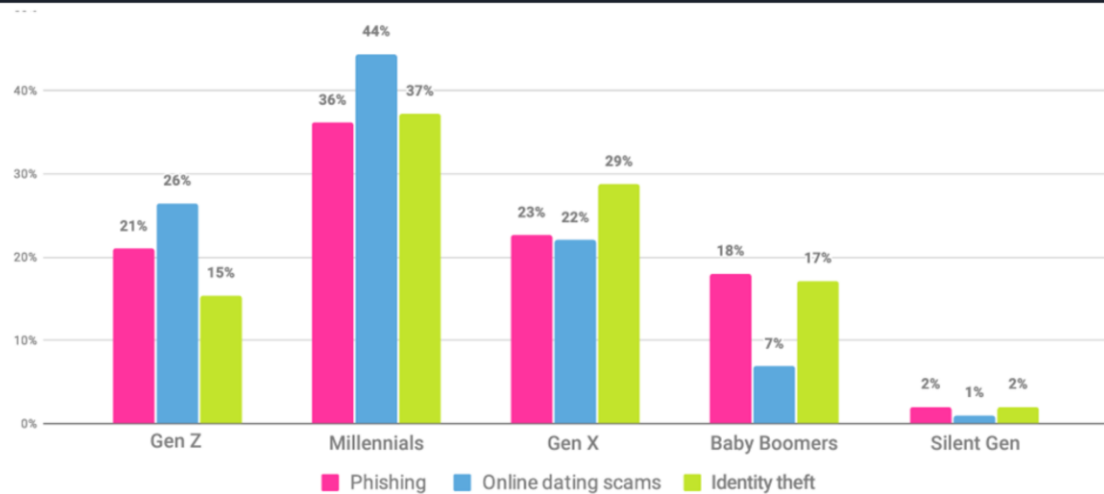


Figure 54. Cybercrime incidents by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime victims: Phishing, 911; Online dating scam, 541; Identity theft, 508 (excluding any cybercrime incidents noted by 316 participants from New Zealand, who didn't provide their age), dates conducted: April 13, 2023 - April 27, 2023.

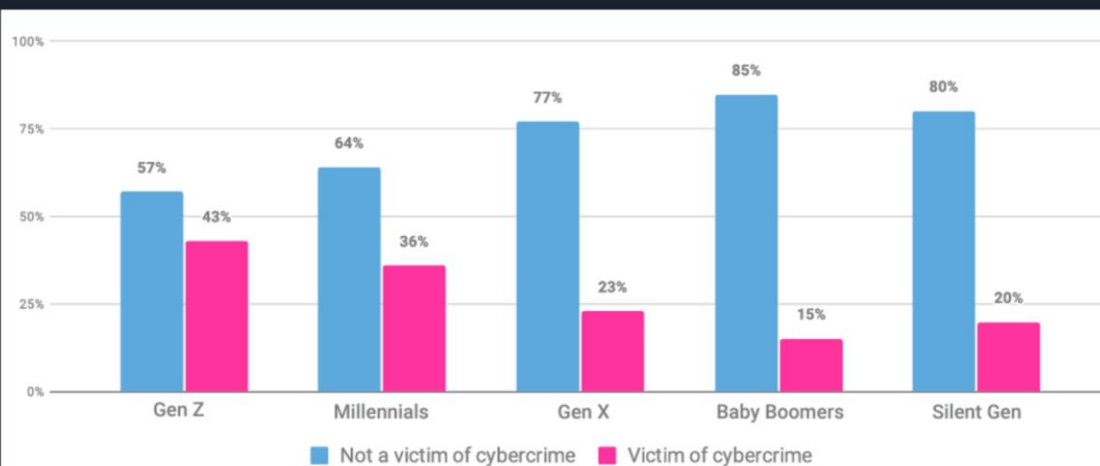
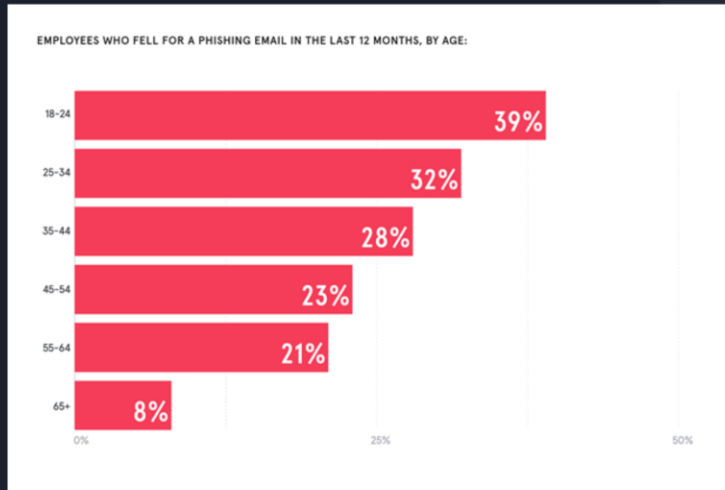


Figure 53. Victimization by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 5748, dates conducted: April 13, 2023 - April 27, 2023.



- Stanford University Professor Jeff Hancock and security firm Tessian report, 2022



UK Pathways Into Cybercrime Report 2017

- 61% begin hacking before age 16
- Skill barrier is low due to off-the-shelf hacking tools
- Start off in game-cheat websites and modding forums and progress to criminal hacking forums
- Financial gain not a priority
- Completing the challenge, sense of accomplishment, proving oneself to peers is key motivation
- Offenders perceive the likelihood of encountering law enforcement as low
- Not anti-social. Online relationships are key. Forum interactions and building reputation.
- Many see criminal hacking as a victimless crime

- UK National Crime Agency – National Cyber Crime Unit




UK Pathways Into Cybercrime Report 2022 - Changes since 2017 Report

- Realistic possibility that the average age of offending and age of initial exposure to cyber crime has fallen since 2017
- It is almost certain that the availability and accessibility of cyber crime tools, especially DDoS for hire and Remote Access Trojans (RATs) have lowered the barrier of entry into cyber crime.

- UK National Crime Agency – National Cyber Crime Unit



- Typical buzzwords associated with cybersecurity
- The human element is missing



References and Resources

- Mitnick, Kevin & Simon, William. The Art of Deception: Controlling the Human Element of Security.
- Mitnick, Kevin. Ghost in the Wires : My Adventures as the World's Most Wanted Hacker.
- Shapiro, Scott J., author. Fancy Bear Goes Phishing : the Dark History of the Information Age, in Five Extraordinary Hacks.
- Cialdini, Robert B. "The Science of Persuasion." Scientific American, vol. 284, no. 2, 2001, pp. 76-81.
- David Gragg. (March 13 2003 SANS Whitepaper) A Multi-Level Defense Against Social Engineering
- Jones, Keith & Armstrong, Miriam & Tornblad, McKenna & Sami Namin, Akbar. (2020). How social engineers use persuasion principles during phishing attacks. Information & Computer Security, ahead-of-print. 10.1108/ICS-07-2020-0113
- Stajano, Frank & Wilson, Paul. (2011). Understanding scam victims: seven principles for systems security. Commun. ACM. 54. 70-75.
- Spinapolic, Matthew, "Mitigating the risk of social engineering attacks" (2011). Thesis. Rochester Institute of Technology.
- W. Zhang, X. Luo, S. D. Burd and A. F. Seazzu. "How Could I Fall for That? Exploring Phishing Victimization with the Heuristic-Systematic Model." 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 2012, pp. 2374-2380, doi: 10.1109/HICSS.2012.302.
- Lively Jr., C. E. (2004). Psychological Based Social Engineering. GIAC practical repository. SANS Institute. <https://www.giac.org/paper/giac/13547/psychological-based-social-engineering/105780>
- Ellis, Jessica (Feb 19, 2019) Brain-hacking: Why Social Engineering is so effective <https://www.phishlabs.com/blog/brain-hacking-social-engineering-effective/>
- Hinton P (2017) Implicit stereotypes and the predictive brain: cognition and culture in 'biased' person perception. Palgrave Communications. 3:17086 doi: 10.1057/palcomms.2017.86. <https://www.nature.com/articles/palcomms201786>
- Preuss, T. M. & Wise, S. P. (2022). Evolution of prefrontal cortex. Neuropsychopharmacology: official publication of the American College of Neuropsychopharmacology, 47(1), 3-19. <https://doi.org/10.1038/s41386-021-00702-3>
- National Crime Agency (NCA) (2017) Pathways into Cyber Crime. National Crime Agency. <http://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file>
- National Crime Agency (NCA) (2021) Pathways into Cyber Crime. National Crime Agency. <http://www.nationalcrimeagency.gov.uk/who-we-are/publications/594-nsc-youth-pathways-into-cyber-crime/file>
- OH BEHAVE! THE ANNUAL CYBERSECURITY ATTITUDES AND BEHAVIORS REPORT 2023. <https://traytafonline.org/online-safety-privacy-basics/oh-behave/>
- Debbi S, Schiffer D, & Colson, D. (2020) A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 42-55. https://www.researchgate.net/publication/355394030_IJCIC-2020-Vol-3-Iss-1
- Cecilia Cheng, Linus Chan, Chor-lam Chau. Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, Volume 108, 2020, 106311, ISSN 0747-5632, <https://www.sciencedirect.com/science/article/pii/S0747563220300650>
- FBI Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- The Psychology of Human Error 2022. <https://www.tandfonline.com/abstract/psychology-of-human-error-2022>
- Mercurio E, García-López E, Morales-Quintero LA, Ullamas NE, Marinero JA and Muñoz JM (2020) Adolescent Brain Development and Progressive Legal Responsibility in the Latin American Context. Front. Psychol. 11:627. doi: 10.3389/fpsyg.2020.00627