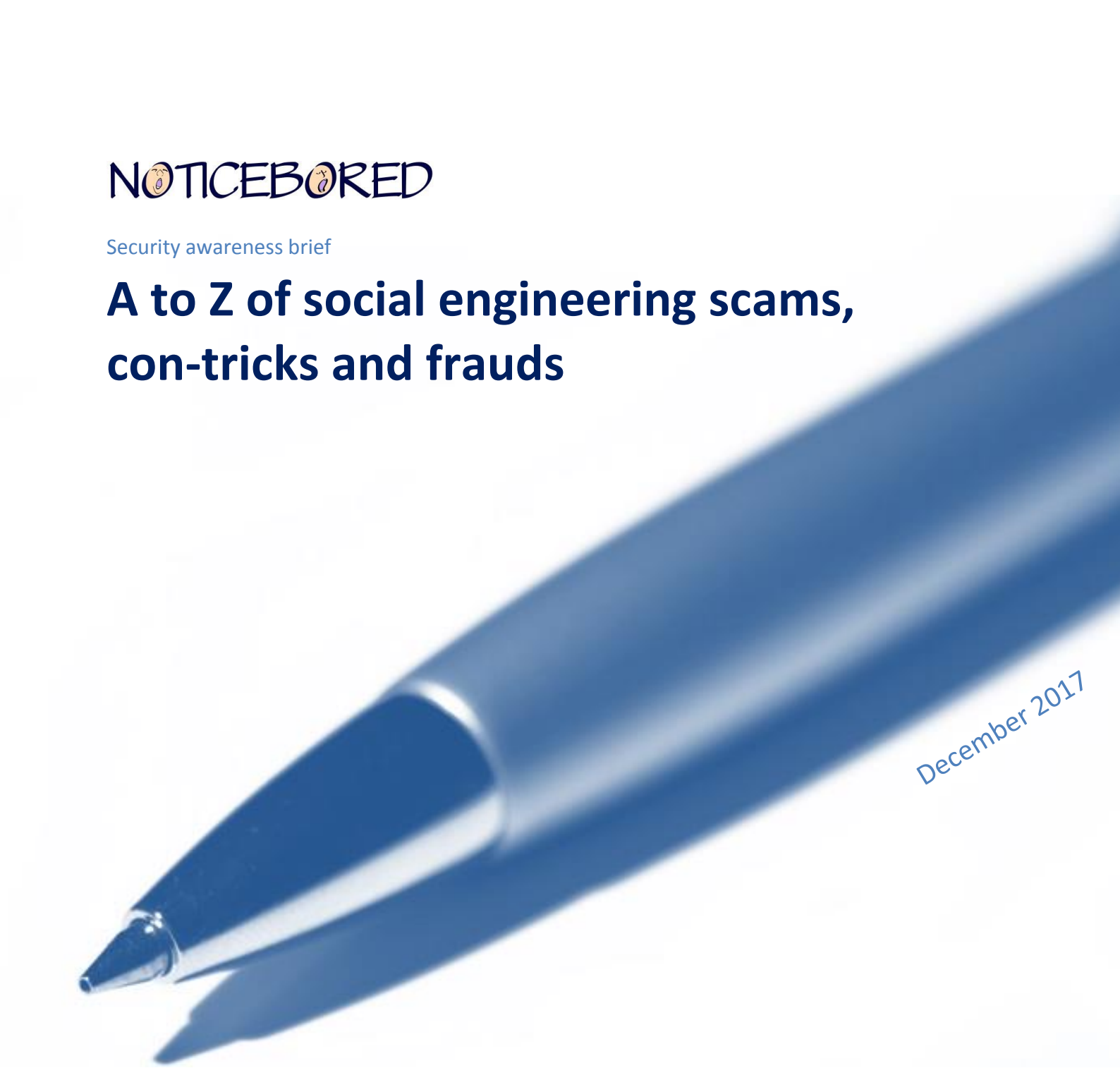
NOTICEBORED

Security awareness brief

A to Z of social engineering scams, con-tricks and frauds



December 2017

Summary

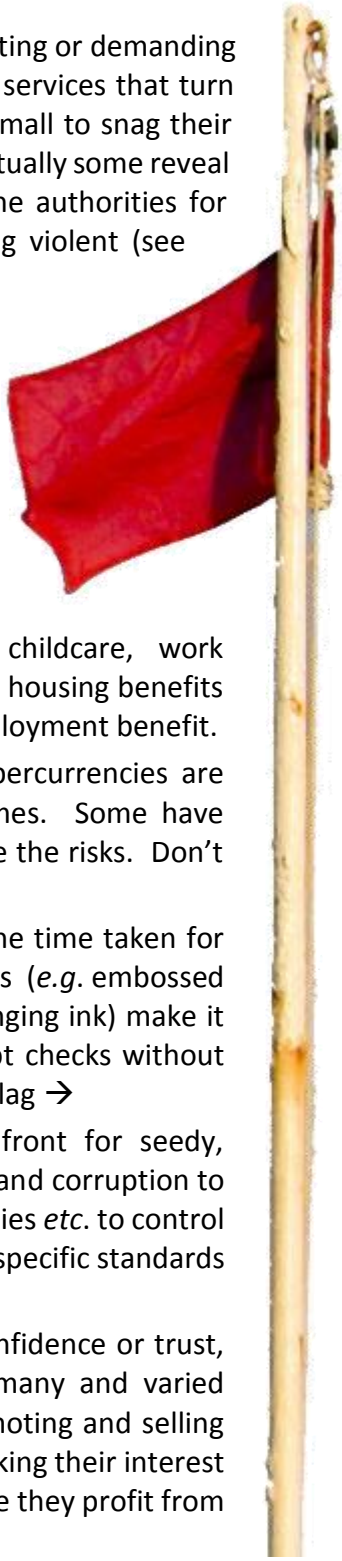
Scammers, con-artists and fraudsters are constantly cooking-up cunning schemes to deceive victims and part them from their valuables. This catalog illustrates the wide variety of threats we face. The content is organized alphabetically but there are *way* more than 26 types. Many have been used for decades, sometimes hundreds or thousands of years (*e.g*. quality and quantity frauds). The details vary though, with numerous wrinkles. Despite the length of this briefing, we're barely scratching the surface of the enormously diverse field of social engineering.

Security awareness briefing

A catalog of social engineering scams, con-tricks and frauds

A **Advance fee ('419') fraud**: this commonplace fraud involves requesting or demanding up-front payments of deposits, charges or other fees for goods or services that turn out not to exist or to be worthless. 419ers are adept at starting small to snag their prey, then gradually upping the stakes as the 'game' proceeds. Eventually some reveal their true nature, perhaps threatening to shop their victims to the authorities for knowingly participating in criminal deeds, possibly even becoming violent (see **killer fraud**). It's not just their thumbs that are screwed.

Auction fraud: various frauds involving auctions, particularly online auctions where buyers and sellers make electronic rather than face-to-face contact *e.g.* non-delivery of goods, goods not as described, counterfeit and stolen goods, shill bidding and phantom bids (fake bids to drive up the hammer price), exorbitant packaging and delivery fees, non- or under-payment, and the use of feedback as a form of coercion.



B **Benefits fraud**: making false or inflated claims for social or corporate benefits for unemployment, housing, healthcare, childcare, work clothing/safety gear *etc.*, for example claiming income support and housing benefits for dead or non-existent relatives, or faking injuries to claim unemployment benefit.

Bitcoin: it is unclear at this point whether Bitcoin and other cybercurrencies are genuine financial instruments, or fraudulent get-rich-quick schemes. Some have collapsed while others flourish. Wise investors diversify to mitigate the risks. Don't say we didn't warn you!

C **Check fraud**: making bogus checks and passing them, exploiting the time taken for the banks to check and clear them. Anti-counterfeiting controls (*e.g.* embossed printing, watermarked paper and temperature sensitive color-changing ink) make it slightly harder to forge checks *provided* recipients refuse to accept checks without them. Someone needs to spot the warning signs and raise the red flag →

Commercial fraud: companies presenting a false but credible front for seedy, disreputable, unethical and criminal organizations; using bribery and corruption to further their business interests; forming cabals, rings, illicit monopolies *etc.* to control the market; excessively restrictive trade practices such as requiring specific standards or trademarks.

Confidence tricks: con-artists exploit victims after gaining their confidence or trust, using that to deceive and manipulate them. Their scams are many and varied *e.g.* 'snake oil salesmen' in the wild West profited by heavily promoting and selling worthless lotions and potions, while modern banks are adept at making their interest rates *appear* attractive for both loans and deposits, a neat trick since they profit from them both!

Counterfeiting: production and sale of fake/pirated goods such as music albums and videos, 'designer label' clothing made in crummy back-street sweatshops, worthless health and beauty products, foods and even pharmaceuticals made from who-knows-what but presented as well-known brands. Intellectual property theft is just part of the scam.

Credit card fraud: use of stolen credit cards or credit card numbers to purchase goods and services, or opening card accounts to obtaining credit using false details.

Cyber fraud: various kinds of fraud involve the use of IT, computers, cellphones, the Internet and other networks and devices as tools to commit/perpetrate and conceal crime. Fraudsters also use IT to run their illegitimate business enterprises, and to communicate with their illicit social networks, to buy and deliver criminal services *etc*. It's the dark side.

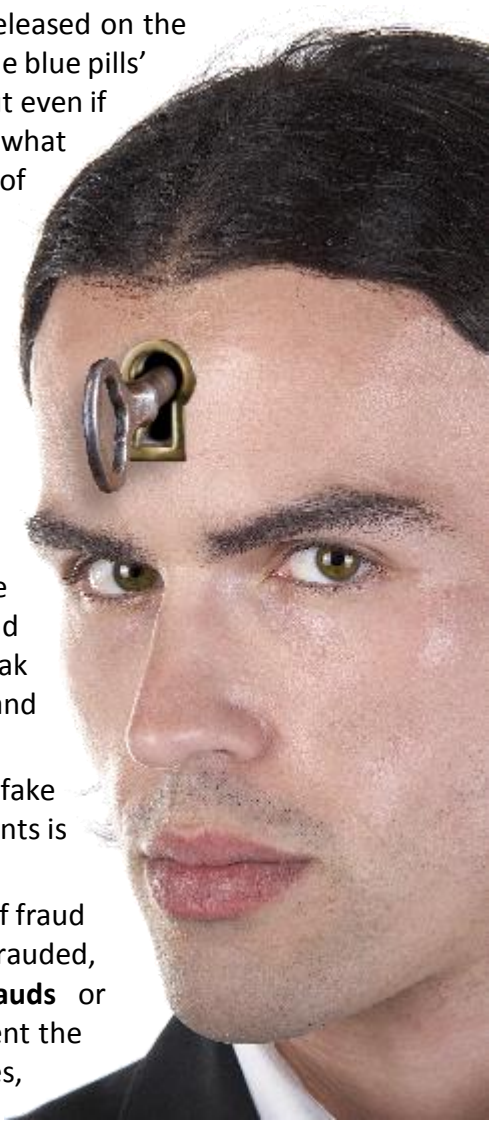
D

Domain name fraud: exploiting naïve businesses by implying that they must pay additional registration fees, directory/search engine listing and private registration fees; or offering low-quality search engine optimization, web design and web hosting services at premium prices; or manipulating domain registrations to redirect emails and web traffic *etc*.

E

Election fraud: vote rigging; gerrymandering; coercion of voters; manipulation of vote recording counting systems and processes … all proof, I guess, that power corrupts.

Erection fraud: a few years back just as Viagra was released on the market, widely circulating spam emails advertised 'little blue pills' and the like, ostensibly to treat erectile dysfunction but even if they worked (the placebo effect again), who knows what they actually contained? From time to time we hear of cocaine cut with bulking agents such as laxative, boric acid, sugar, milk powder … or rat poison (**quantity and quality fraud**).



Expenses fraud: fabricating or inflating expenses claims for things that were not in fact legitimate business expenses, including overcharging customers by submitting fake or modified receipts on 'cost-recovery' or 'chargeback' contracts (the dodgy builders' favorite!).

Export fraud: scams exploiting various loopholes in the rules and regulations, plus the process, of exporting and importing goods *e.g.* taking advantage of weak compliance checks, lax or differing product standards and differing tax laws.

F

Fake news: deliberately fabricating and circulating fake news items to discredit opponents and boost proponents is an ancient practice, also known as propaganda.

Fraud recovery fraud: a particularly despicable form of fraud that preys on people who have already been defrauded, typically losing money to **advance fee (419) frauds** or **ransomware**. The fraudsters usually claim to represent the authorities or lawyers investigating the earlier offenses, and offer to help victims recover lost funds or claim

compensation … but almost immediately they start demanding payments for bogus expenses starting a further round of advance fee fraud, targeting those who are patently naïve and vulnerable.

Go-large fraud: "Would you like fries with that?" is an appeal to your hunger/greed *and* the fast food outlet's profits. So-called super-sized meals and optional extras in general can make the difference between the vendor making a loss or turning a profit. Psychologically speaking, the customer has swallowed the hook at the point the question is posed, having already made the key purchase decision.

> Add-ons – optional extras - are not subject to the same scrutiny and care as the base purchase, and often (but not always) represent poor value for money. The pressure to 'upgrade' can be quite subtle but relentless: would *you* settle for, say, second-best health care? What about second-rate education for your children, or sub-standard 'retirement care' for your parents? Fancy a little more leg-room, a "free" video and maybe a better meal on the plane? Can you not *afford* a slightly bigger or fancier home in a more up-market area?

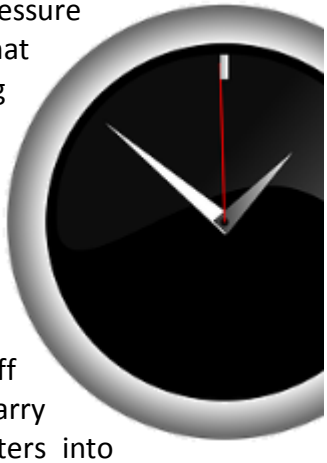
Health-related fraud: faking illness or injury, deliberately 'taking a sickie' (possibly using fake sick notes); inflating reclaimable medical expenses or obtaining prescription medicines to sell on the black market; charlatans pushing snake oil, making false claims for the effectiveness of the products they sell, cynically exploiting the sick and desperate …

Homeopathy: one of many **health-related frauds** based on a grain of truth. Homeopathic remedies are typically so far diluted that no chemical trace of the supposed active ingredient remains – not a single atom – and yet some customers *believe* them effective … and that *belief* may itself be therapeutic. In conventional medicine, this is known as the placebo effect. Is it fraud if your health improves as a result of spending a small fortune on what amounts to a bottle of water with a fancy label? There are many other dubious 'treatments', 'supplements', 'supports', 'remedies' *etc*. plus devices (such as magnets, copper bracelets and magic crystals), that work on a psychosomatic rather than physical, chemical or biological level. Some (including some herbal products) may have genuinely beneficial biological effects, and some (including some herbal products) can be dangerous.

Identity fraud: commonly but incorrectly called "identity theft", the fraudster masquerades as the victim in order to steal the victim's assets, exploit their reputation *etc*. This may be as easy as guessing a short, weak password, or tricking someone into revealing their passphrase *e.g*. by **phishing** or spyware.

Insurance fraud: making false or inflated insurance claims, or deliberately compromising insured goods (*e.g*. "spilling" paint on a carpet, committing arson or leaving a vehicle exposed in a public place with the door/window open and maybe the keys in the ignition).

International fraud: fraud involving organizations or individuals from different countries, taking advantage of physical, cultural, ethical and legal differences plus physical distance, plus ineffective enforcement by the authorities in some countries (resulting in part from lack of resources, plus fraud and corruption – backhanders to officials, and a tolerance for crimes exploiting foreigners).



J

Just-in-time fraud: many scams and frauds deliberately pressure recipients into making snap decisions, for example by claiming that their action is urgently required to prevent their account being closed, or to claim a refund or discount, or to help a colleague in trouble. The hope is that victims won't take the time to think clearly and check the details, but will make payments straight away, before the banks and authorities are able to identify the frauds and disrupt the money laundering mechanisms.

K

Killer fraud: fraudsters sometimes masquerade as hired guns, trained killers under contract to kill their victims unless they pay off some alleged debt or protection money … and occasionally they carry through on their threats. Victims have been lured by fraudsters into dangerous situations (*e.g.* visiting West Africa supposedly to collect their fake inheritance payouts, diamonds or gold dust) and attacked, held hostage and sometimes killed. The organized criminals behind many of the schemes are neither law-abiding nor compassionate. We are indeed 'fair game' to them.

L

Legal fraud: leaving aside frauds perpetrated by lawyers and others within the legal system (which may or may not be legal), some relatively trivial forms of fraud are not expressly forbidden in law and, it seems, are widely tolerated by society. We've noted a few in this A-to-Z. Depending on one's perspective, things such as **fake news** and **homeopathy** may be fraudulent, trivial scams, 'obvious' parodies, 'a stretch of the truth', misrepresentation, misleading and unethical … or conversely persuasive, ethical, legitimate and beneficial. A few, such as **M**ulti **L**evel **M**arketing sit right on the cusp: even trained professionals who analyze them in detail cannot always determine whether they are ethical or unethical, legal or illegal. Such is the ambiguous nature of frauds, con-tricks and scams, and social engineering in general.

Lonely heart scams: scammers prey on lonely people looking for love, offering a friendly ear, support, companionship, sex or whatever it takes to gain their confidence, form a relationship and drop their guard … before exploiting them in some way. **Advance fee frauds** are common, plus identity fraud and straightforward theft of the person's assets. Sometimes the aim is to get married in order to qualify for a visa or work permit. It cuts both ways though: sometimes the scammers are the ones being victimized.

Lottery fraud: we may dream of receiving a message along the lines of 'It's your lucky day! Your email has been drawn and you have won $13.7 million (thirteen million seven hundred thousand dollars)' but virtually all of them are fraudulent, often **advance fee frauds** or **identity frauds**. If you honestly expect to have won a lottery you didn't even enter, well maybe P.T. Barnum had it right: "There's one born every minute."

M

Mail fraud: essentially, any fraud involving use of the postal mail system to deliver fraudulent or illegal materials (*e.g.* misleading pamphlets, bogus checks, drugs), or where the postal system itself is an integral part of the fraud (*e.g.* getting letters and parcels containing fraudulently obtained goods, credit cards *etc.* delivered to a mail drop address in order to conceal the fraudster's location, or secretly redirecting someone's mail in order to intercept or steal it).

Marketing fraud: there's a fine line between honestly promoting the genuine advantages to customers of a product, and inflating them. The latter issue has dogged the IT market for decades, convincing customers to buy hardware and software packages that (in some cases) don't exist, fail to do what they promise, or suffer from design flaws, bugs, incompatibilities and (all too often) security vulnerabilities.

N

Novel frauds: no, this is not about misleading best-sellers – it's about genuinely new forms of fraud. Most are variants of existing, well-known ones but occasionally someone comes up with a totally novel way to mislead, manipulate and exploit people. Spotting the new ones is especially hard because they are *designed* to deceive, to appear normal, indefinitely if possible. Victims may *never* realize they have been taken for a ride.

O

Online fraud: the Internet is a fabulous tool of the fraudster's trade. It allows them to reach vast numbers of potential victims easily at near zero cost and risk, to research individuals and frauds, to launder the proceeds or use various criminal cloud services (such as botnets – networks of compromised computers available to rent for delivering viruses, spam *etc*.). Traditional offline fraud tends to be costlier and riskier for the fraudsters, but can be very lucrative (*e.g*. **tax fraud**) and is unlikely to die out.

P

Penetration testing and auditing: social engineering techniques are sometimes employed in legitimate and authorized penetration tests, audits and other security tests, checking that workers spot and respond appropriately … and occasional we hear of enterprising social engineers using that pretext to justify and explain away their activities when challenged. "I'm from audit. Look, here's my pass, and my access-all-areas letter from the CEO. Now, tell me everything you know … including your password as I need to check your network access …" [Either way, an appropriate response would be "Hold on a moment, stop right there. Let me check that out. If you breathe too loudly, I'll be calling Security … in fact my colleague over there is already on the phone to them …"]

Phishing: faking emails, text messages *etc*. trick victims into trusting the sender and doing something inappropriate - typically revealing their usernames and passwords in **identity fraud**, or giving access to sensitive systems and data, perhaps even opening the door.

Pyramid schemes also known as **Ponzi schemes**: mostly these rely on people paying to join up, their money being paid out to members already on board which is the main draw. As the schemes grow larger, the payouts are distributed more widely, requiring even more new joiners to fund the promised payouts … until eventually the flow of new joiners dries up and the schemes inevitably collapse, leaving all recent joiners and many more out of pocket.

Political/governmental fraud: bribes/inducements or fees paid or received by corrupt politicians in return for political favors; manipulating information and making false claims on the government's record, policies *etc*.; digging out or generating, exaggerating and spreading scurrilous rumors about members of the opposition; leaking harmful information to the media or pressure groups; misusing the power of office to suppress the opposition; election fraud.

Procurement fraud: buyers collude with sellers to make their employers pay false or inflated invoices for goods and services that were not legitimately supplied, or to select suboptimal suppliers and products (in return for a bribe from the supplier).

Q

Quality and quantity frauds: these involve substituting inferior products for those advertised and ordered, or delivering short measures of any product sold by weight or volume or time (*e.g.* the lawyer's services). Each delivery may only be a little short (perhaps within the leeway known euphemistically as "natural variation", "settlement", "measurement tolerance" or "rounding"), but gradually it mounts up – a form of salami fraud.

Have you noticed how the grinning small-handed customers in hamburger ads grab their burgers with both hands, holding them close to the camera to make them seem huge in perspective? So how do you feel when the burger you've ordered turns out in fact to be a sad, pasty little bun with a slab of mechanically recovered 'meat', loads of cheap lettuce and onion, far too much salt and strong sauce to combat the general lack of flavor? Is that powerful and effective marketing, good business, or quality and quantity fraud?

Qualifications fraud: want a degree? Sure, why not! Simply buy one! Not quite good enough to make the grade as a professional? No worries: become an associate and we will uprate you to full membership after a few months or years. Need to sound competent at something? We can supply an authentic certificate with your name embossed upon it in gold foil. Simply wire us your money …

R

Racketeering: 'protection rackets', for instance, pressure victims into paying handsomely for various security services that are not, in fact, required, to protect them against (other) criminals, competitors, authorities and adversaries.

Ransomware and scareware: whereas most computer viruses do their utmost to remain hidden, when the time is ripe some display scary warning messages, generally accompanied with a demand for money. The warning may be genuine (*e.g.* ransomware may actually have scrambled the user's data) or baseless (*e.g.* scareware merely *claiming* to have scrambled the user's data): either way the user may be pressured into paying up.

Résumé fraud: while it is generally expected that job applicants emphasize their good points and downplay the bad in their résumés, the more desperate and less ethical among us have been known to fabricate employment histories – for example inventing a fake job with a nonexistent or now defunct employer, perhaps citing 'references' that cannot be contacted, to cover a period actually spent on the run or in prison.

S

Salami fraud: taking and accumulating such thin 'slices' of something valuable (such as interest on a bank account, email addresses in an email system, or rounding errors in an accounting system) that they remain unnoticed. Given enough slicers in action over a sufficiently long period, it is possible for salami fraudsters to accumulate a tidy stack of valuables … unless they are caught red-handed anyway, smelling of meat.

Sales fraud: selling goods at a knock-down price to accomplices (possibly for re-sale at the usual price, pocketing the difference) or falsifying sales records to over-claim commission, bonuses and over-state profits, or to under-pay sales and income taxes.

Stock frauds: conning naive investors into investing in nonexistent, highly risky and/or over-priced companies, including so-called penny stocks, using high-pressure sales techniques ('boiler-rooms') and the promise of huge returns.

Tax and accounting frauds: too many to count! Some unethical tax advisors and accountants specialize in finding and exploiting loopholes in the laws and regulations, or weaknesses in the authorities' detection and enforcement activities, encouraging and facilitating their clients to push or break legal constraints and boundaries. Meanwhile, the authorities do their best to close the loopholes, design and implement controls, tighten-up the legislation and enforcement, and locate and prosecute offenders, all the time increasing costs … which are paid by law-abiding taxpayers, adversely affecting the nation as a whole. Tax cheats and dodgy accountants are society's parasites.

Timesheet fraud: hourly- or daily-paid workers (including professionals such as plumbers, lawyers, accountants, doctors and vets) who inflate or fabricate their timesheets to overcharge clients or employers. This is a variant of quantity fraud, often with a dose of quality, expenses and tax fraud thrown in for good measure!

Unmitigated fraud: aside from novel and as-yet unrecognized frauds, many relatively minor con-tricks and scams remain largely unmitigated, that is neither prevented nor reduced by any specific controls, in effect being tolerated by society. The main reason is economic: it would cost more to address them than doing so would save. It's not always clear who is responsible for taking action, and exactly what action to take. The upshot is that *we*, the people, need to look after our own interests.

This awareness briefing is meant to open your eyes to the possibilities and put you on guard. When it comes to social engineering in all its glory, we can't entirely rely on technology to keep us out of trouble. **The organization *needs* our vigilance!**

Victimless fraud … is a myth. When a person or organization is tricked in some way, deceived into giving up some asset or advantage, those are costs borne by the person or organization directly, or transferred onto their families, customers and the general public. Tax fraud is a classic example: when, say, a customer pays a tradesman in cash to avoid putting it through the books and accounting for the sales tax due, that reduces the revenue paid into the treasury. It may not be a lot of money but it all adds up (much like a salami fraud perpetrated by the taxman)! On top of that, the authorities have to invest in controls to mitigate such frauds, for instance identifying and checking-up on people who are evidently 'living beyond their means'.

Wine fraud: for example blending or substituting lower-grade grapes and wines for those ordered, mis-labeling bottles and cases, artificially aging the labels faking older vintages, watering down the wine *etc*. Even the shape of the bottle can be changed to make it *appear* larger and hence better value! When was the last time you checked that a bottle of wine actually contained no less than the volume printed on the label?

X e**X**treme fraud: occasionally we hear about particularly devastating frauds, often conducted on a massive scale by groups with strong criminal connections and (most likely) support from people working for the organizations expected to protect their victims. The Enron scandal, for instance, made some people ridiculously rich, others very poor, and led to the downfall of the corporate auditors who were observed, near the end of the debacle, desperately shredding paperwork presumably containing evidence of their shenanigans. As this is being written, wild stories are emerging of the excesses of Robert Mugabe of Zimbabwe, who is *alleged* to have been involved in widespread bribery and corruption, a problem endemic across Africa and beyond. We may never know the truth of it.

Y **Yahoo! fraud**: perhaps it's unfair to single-out Yahoo! since Yahoo!, Gmail and many similar email addresses are readily obtained for free with next to no authentication of a person's identity, making them more or less anonymous and hard to trace, a convenient means of covert communication valued by scammers, con-artists and fraudsters.

Z **Zero fraud:** an extremely common one this. Instead of selling products at a round number price point such as $10, they are priced a little lower to take advantage of the perception that, say, $9.99 is "nine dollars and small change", as well as being legitimately promoted as "under ten dollars". Subconsciously, the customer is hoodwinked into focusing on the nines rather than thinking of it as nearly-ten. The effect is stronger the further the retailers depart from the round number, for example $9.89 is conceptually 'considerably less' than $10, despite the difference being just 1.1% in fact. If a customer pays with a $10 bill and their change is rounded down as well, the price paid may be just 1% less than $10, yet somehow research shows that it's a curiously effective pricing strategy. Whether you consider it fraud or just good business is a moot point: either way, customers are deliberately misled.

Your responsibilities

Social engineering attacks, scams, con-tricks and frauds are of concern to the organization, as well as to us individually plus our families and friends. Fraudsters, for instance, may target individual workers as a way to gain control of the corporate bank accounts. Hackers often utilize social engineering methods to gather technical information and, more directly, to gain access to corporate IT networks and systems.

We are doing all we can to harden and secure the technology against technical attacks. We need *your* help, though, to protect our people against the non-technical attacks described in this A-to-Z. Having read this briefing, you are now aware of the challenges we face. We ask you, please, to remain vigilant and report social engineering attacks to the Help Desk.

Other security awareness materials provide further practical guidance, for example the **DART** method to **D**elay, **A**uthenticate, **R**esist and **T**ransfer suspected social engineers.

We're counting on YOU!

Further information

Browse the intranet *Security Zone* or call the Help Desk for assistance.

NOTICEBORED

This briefing is just *part* of an integrated suite of security awareness materials and activities on social engineering, our information security topic for December 2017.

NoticeBored subscribers receive the customizable MS Word version of this paper, along with other awareness materials on social engineering such as PowerPoint slide decks, high-res posters and Visio mind maps, a quiz and test, a comprehensive glossary, management-level content including policy templates, metrics and checklists, and more in-depth awareness/training materials for professionals. We are currently working on complementary A-Z guides on social engineering methods and controls. December's NoticeBored module is a cracker!

Social engineering is a vital topic for any security awareness program … but there are many others too. Our portfolio covers more than 60 information security topics giving a different focus and something fresh every month, supporting year-round awareness and security culture.

Thank you for your interest in our services. For more information, please see www.NoticeBored.com and the NoticeBored blog, or email me: Gary@isect.com.

Kind regards,
Gary Hinson, CEO IsecT Ltd., New Zealand