ALL Y'ALL, WE LOVE LIMITED BALLOTS.

```
01001001 00100000 01110101 01110011
01100101 01100100 00100000 01110100
01101111 00100000 01110011 01100001
01111001 00100000 01110100 01101000
01100001 01110100 00100000 01110000
01101111 01101100 01101001 01110100
01101001 01100011 01110011 00100000
01110111 01100001 01110011 00100000
01110100 01101000 01100101 00100000
01110011 01100101 01100011 01101111
01101110 01100100 00101101 01101111
01101100 01100100 01100101 01110011
01110100 00100000 01110000 01110010
01101111 01100110 01100101 01110011
01110011 01101001 01101111 01101110
00101110 00100000 01001001 00100000
01101000 01100001 01110110 01100101
00100000 01100011 01101111 01101101
01100101 00100000 01110100 01101111
00100000 01101011 01101110 01101111
01110111 00100000 01110100 01101000
01100001 01110100 00100000 01101001
01110100 00100000 01100010 01100101
01100001 01110010 01110011 00100000
01100001 00100000 01100111 01110010
01101111 01110011 01110011 00100000
01110011 01101001 01101101 01101001
01101100 01100001 01110010 01101001
01110100 01111001 00100000 01110100
01101111 00100000 01110100 01101000
01100101 00100000 01100110 01101001
01110010 01110011 01110100 00101110
00100000 00000000 00000000 00000000
00100000 01010010 01101111 01101110
01100001 01101100 01100100 00100000
01010010 01100101 01100001 01100111
01100001 01101110
```

Oct 19 2020

Vote Early, Vote Often, Vote to PWN :)

Limited Ballot Zero-day Vulnerability!

Commandeering the election because our agenda is more important.

all y’all, we love limited ballots.

VOTE EARLY, VOTE OFTEN, VOTE TO PWN :)

History: 2005 from the 79th Session HB 2454 would allow a registered voter who has resided in a new county for less than 90 days to vote a limited ballot. Early voting only!

Limited ballots allow **only early voters** registered in a county different from their current residence to vote after the registration deadline has passed. After filling out an affidavit, the voter will receive a ballot with the races they are eligible to vote for. Once the voter turns in the ballot, they are asked to complete a registration form in the new county. Their previous registration is canceled, and their new registration then is processed.

Limited ballots bypass the provisional ballot safeguards of isolating a ballot for review and verification or rejection. Here is the history of that change:

> *2003 legislature passed Help American Vote Act (HAVA). The most significant change in this legislation for Texas is moving from the current system of challenge ballots to one of provisional ballots. This means that any ballot cast by voters who can't prove (by affidavit) that they are registered, would go to a board that would determine if the ballot should be counted. The bill contains detailed procedures for determining eligibility, how ballots are handled, how they are counted, disposition, etc.*

While Election Judges and Clerks are well-trained before the early vote begins, the Election Advisories may be presented to the Judge at the start of early voting, typically a half hour before the polls open or when an issue of election law comes to the forefront. Due to information overload and the pressure of opening the polls on time, Election Advisories are typically set aside for review during a down time. Election Advisories can also cause confusion that requires the Secretary of State (SOS) attorneys division to review and then a follow-up call, adding to the timeline.
This creates an attack vector in the process that can be exploited by a Threat Actor. To exploit vulnerabilities, an attacker must have at least one applicable tool or technique that can exploit a weakness. Confusion, conflicting laws, time gaps in detection, are some of the weaknesses.

TYPES OF THREAT ACTORS THAT HAVE A DESIRED POLITICAL OUTCOME:

State-Sponsored Election Attackers: objectives aligned with their political interests of their country of origin. A State-Sponsored Actor is going to persist in their victim’s election, without their knowledge or noticeable impact, for months to years before discovery. Limited ballots are typically counted after Early Vote is over and the successful attack cannot be backed out.

Hacktivists: are generally not motivated by money. Instead, they have an inflamed rage that, for whatever social reason, has been directed at a given political party or candidate. “The end justifies the means” drives their appetite for results without any regard for risk or collateral damage.

THREAT ACTOR PASSIVE RECONNAISSANCE:

Months before the election, information gathering and the data collection about the early vote process would begin. Detailing all the processes, procedures, required forged documents and timelines to carry out the early vote attack, without engaging the actual target. Here are a few examples.

1. Reading research.
   a. **Sec. 63.001. REGULAR PROCEDURE FOR ACCEPTING VOTER**. Section (c-1) provides an opening.
   b. **Sec. 112.002 ELIGIBILITY, in the Texas election code.**
   c. **Election Advisory No. 2018-32** Date: October 9, 2018 and the weak statement of "must attempt".
   d. Affidavit for Limited Ballot. https://www.sos.state.tx.us/elections/forms/pol-sub/5-28f.pdf
2. County with paper or optical scan and a population below 100,000 is a softer target. Voting equipment is expensive and small population counties do not have a budget to upgrade equipment regularly. Search the county's commissioner court minutes to see if they have upgraded the equipment for this election cycle. Lowers the risk of getting caught.
3. Valid voter who had died after the last day to register and before Early Voting period (12 day window). Funeral home data is available online and a simple search in the obituary section provides a wealth of information including age of the identity to assume, which helps to find a close match for the new false ID.
4. Use a people search engine to verify the new identity with the family members to get a current address crosscheck with some of the names harvested from the obituary. Check if any relatives live in the targeted county, which would negate the use of certain ID's. Also use Google/Bing or a law enforcement database to make sure the person was not a current convicted felon.
5. Call the elections office in the source county, ask for the voter registration number of the acquired ID or use one of the lists from the political parties. If asked why you need the voter ID, tell them you are verifying ID's for a petition they signed.
6. Create a false voter registration card and compare agents a valid voter card to match style and authenticity.
7. Create a paper DPS license for picture ID requirement. Add an endorsement for the reason of paper ID.
8. Fold/wrinkle both the Voter Registration Certificate and the paper forged DPS ID, to corrupt the bar code and license number, requires the clerk to type in the information and reduces the risk of the computer catching the forgery with imaging software.
9. Four (4) random numbers for the SSI section in "Affidavit for Limited Ballot", to be used instead of the DPS ID number. Nothing more than "Security Theater" as it may never get properly verified, but it looks scary official.

EXECUTIONS OF IN-PERSON ZERO-DAY LIMITED BALLOT EXPLOIT SCENARIO:

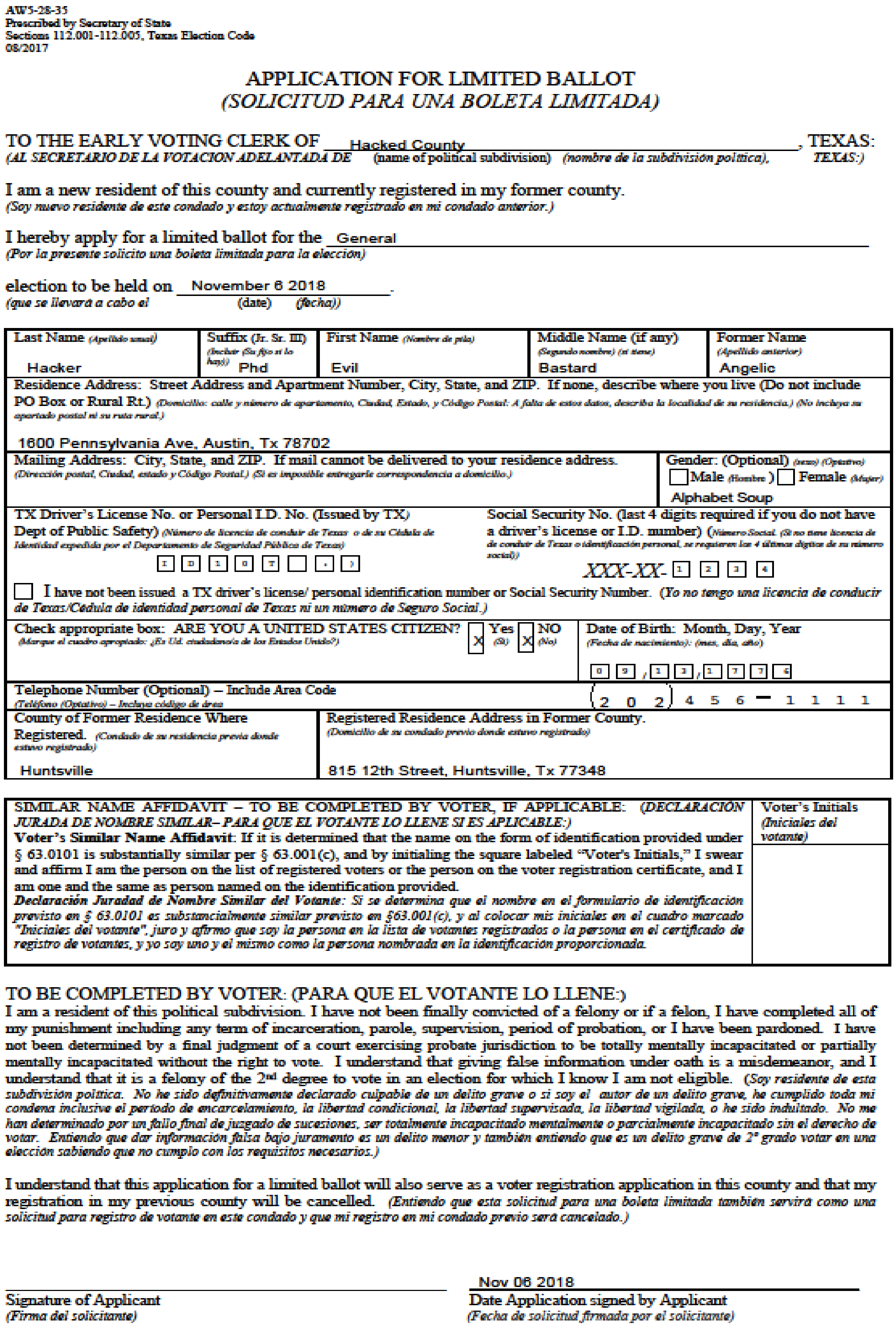
We will use a small Texas county with a population of approximately 50,000 as an example, as they average a 4 hour or greater gap in updating "Limited Ballot Affidavits" to the State Database, which creates another vulnerability to exploit.

Threat Actor enters the polling place with a few people in line, and more people walking up, an easy way to blend in. With more voters entering the line behind the Actor it will place social pressure on the Judge and Clerks to expedite the Limited Ballot voting process while helping other voters.

THREAT ACTOR (FRAUDULENT VOTER) ENTERS SOCIAL ENGINEERING PHASE AGAINST THE ELECTION CLERK/JUDGE:

- Actor "I just moved to the RV Park. I don't know the address and will be moving in December to the next oil rig in Midland as I am a pipe-line welder. The RV Park is on I-20 between the cities of Canton and Van on the south side. You probably know the place and can look up the address. The Dallas radio station said something about a half ballot."
- Clerk replies, "Oh, you mean a Limited Ballot."
- Actor replies, "Yeah that is probably what the dude on the radio said. So what do you need from me so that I can vote the partial ballot?" Keeping the clerk off balance, the Actor feigns ignorance about Limited Ballots, and Clerk now puts the Actor into "Low Information Voter" category.
- Clerk asks the Actor for a picture ID.
- Actor says, "I have this paper one from DPS but it's all wrinkled and been in my pocket", but you can see my picture. (Actor made sure not all the numbers are visible).
- Clerk asks the Actor for a "voter registration card".
- Actor says, "Yep this is where I used to live, you can look up that I have voted in the past."
- Clerk says to the Actor, "Looks like you can vote but you have to fill out the 'Affidavit for Limited Ballot', then you can vote a Limited Ballot once we mark out the races you can't vote in."
    - Note: the District Chart is 86 pages with 254 counties; the Clerk has to determine the overlap of races that the voter can vote in.

- Actor while filling out the "Affidavit for Limited Ballot" asks the clerk "Will I be able to vote for candidate X over candidate Y?" in a loud voice so other voters can hear.
- Clerk asks the Actor to keep her voice down and notices the line is getting longer.
- After the affidavits are signed the clerk hands the Actor a Limited Ballot.
- Actor brings back the illegally voted ballot to the Clerk and says, "I want my vote to count for candidate X, where does it go?"
- Clerk says, "Your ballot is placed in a separate election box to be hand-counted by the Early Ballot Board. Have a nice day and please leave quietly."
- Actor knows there is time to still pull off the same hack in three (3) more counties.



AW5-28-35
Prescribed by Secretary of State
Sections 112.001-112.005, Texas Election Code
08/2017

APPLICATION FOR LIMITED BALLOT
(SOLICITUD PARA UNA BOLETA LIMITADA)

TO THE EARLY VOTING CLERK OF Hacked County, TEXAS:
(AL SECRETARIO DE LA VOTACION ADELANTADA DE (name of political subdivision) *(nombre de la subdivisión política), TEXAS:)*

I am a new resident of this county and currently registered in my former county.
(Soy nuevo residente de este condado y estoy actualmente registrado en mi condado anterior.)

I hereby apply for a limited ballot for the General
(Por la presente solicito una boleta limitada para la elección)

election to be held on November 6 2018.
(que se llevará a cabo el (date) *(fecha))*

Last Name *(Apellido usual)* Hacker	Suffix (Jr. Sr. III) *(Incluir (Su fijo si lo hay))* Phd	First Name *(Nombre de pila)* Evil	Middle Name (if any) *(Segundo nombre) (si tiene)* Bastard	Former Name *(Apellido anterior)* Angelic

Residence Address: Street Address and Apartment Number, City, State, and ZIP. If none, describe where you live (Do not include PO Box or Rural Rt.) *(Domicilio: calle y número de apartamento, Ciudad, Estado, y Código Postal: A falta de estos datos, describa la localidad de su residencia.) (No incluya su apartado postal ni su ruta rural.)*
1600 Pennsylvania Ave, Austin, Tx 78702

Mailing Address: City, State, and ZIP. If mail cannot be delivered to your residence address. *(Dirección postal, Ciudad, estado y Código Postal.) (Si es imposible entregarle correspondencia a domicilio.)*

Gender: (Optional) *(sexo) (Optativo)*
□ Male *(Hombre)* □ Female *(Mujer)*
Alphabet Soup

TX Driver's License No. or Personal I.D. No. (Issued by TX Dept of Public Safety) *(Número de licencia de conducir de Texas o de su Cédula de Identidad expedida por el Departamento de Seguridad Pública de Texas)*
I D 1 0 T ;)

Social Security No. (last 4 digits required if you do not have a driver's license or I.D. number) *(Número Social. (Si no tiene licencia de de conducir de Texas o identificación personal, se requieren los 4 últimos dígitos de su número social))*
XXX-XX- 1 2 3 4

□ I have not been issued a TX driver's license/ personal identification number or Social Security Number. *(Yo no tengo una licencia de conducir de Texas/Cédula de identidad personal de Texas ni un número de Seguro Social.)*

Check appropriate box: ARE YOU A UNITED STATES CITIZEN? ☒ Yes *(Sí)* ☒ NO *(No)*
(Marque el cuadro apropiado: ¿Es Ud. ciudadano/a de los Estados Unido?)

Date of Birth: Month, Day, Year
(Fecha de nacimiento): (mes, día, año)
0 9 / 1 3 / 1 7 7 6

Telephone Number (Optional) – Include Area Code
(Teléfono (Optativo) – Incluya código de área
(2 0 2) 4 5 6 – 1 1 1 1

County of Former Residence Where Registered. *(Condado de su residencia previa donde estuvo registrado)*
Huntsville

Registered Residence Address in Former County. *(Domicilio de su condado previo donde estuvo registrado)*
815 12th Street, Huntsville, Tx 77348

SIMILAR NAME AFFIDAVIT – TO BE COMPLETED BY VOTER, IF APPLICABLE: *(DECLARACIÓN JURADA DE NOMBRE SIMILAR– PARA QUE EL VOTANTE LO LLENE SI ES APLICABLE:)*
Voter's Similar Name Affidavit: If it is determined that the name on the form of identification provided under § 63.0101 is substantially similar per § 63.001(c), and by initialing the square labeled "Voter's Initials," I swear and affirm I am the person on the list of registered voters or the person on the voter registration certificate, and I am one and the same as person named on the identification provided.
Declaración Juradad de Nombre Similar del Votante: *Si se determina que el nombre en el formulario de identificación previsto en § 63.0101 es substancialmente similar previsto en §63.001(c), y al colocar mis iniciales en el cuadro marcado "Iniciales del votante", juro y afirmo que soy la persona en la lista de votantes registrados o la persona en el certificado de registro de votantes, y yo soy uno y el mismo como la persona nombrada en la identificación proporcionada.*

Voter's Initials *(Iniciales del votante)*

TO BE COMPLETED BY VOTER: (PARA QUE EL VOTANTE LO LLENE:)
I am a resident of this political subdivision. I have not been finally convicted of a felony or if a felon, I have completed all of my punishment including any term of incarceration, parole, supervision, period of probation, or I have been pardoned. I have not been determined by a final judgment of a court exercising probate jurisdiction to be totally mentally incapacitated or partially mentally incapacitated without the right to vote. I understand that giving false information under oath is a misdemeanor, and I understand that it is a felony of the 2nd degree to vote in an election for which I know I am not eligible. *(Soy residente de esta subdivisión política. No he sido definitivamente declarado culpable de un delito grave o si soy el autor de un delito grave, he cumplido toda mi condena inclusive el período de encarcelamiento, la libertad condicional, la libertad supervisada, la libertad vigilada, o he sido indultado. No me han determinado por un fallo final de juzgado de sucesiones, ser totalmente incapacitado mentalmente o parcialmente incapacitado sin el derecho de votar. Entiendo que dar información falsa bajo juramento es un delito menor y también entiendo que es un delito grave de 2° grado votar en una elección sabiendo que no cumplo con los requisitos necesarios.)*

I understand that this application for a limited ballot will also serve as a voter registration application in this county and that my registration in my previous county will be cancelled. *(Entiendo que esta solicitud para una boleta limitada también servirá como una solicitud para registro de votante en este condado y que mi registro en mi condado previo será cancelado.)*

Signature of Applicant
(Firma del solicitante)

Nov 06 2018
Date Application signed by Applicant
(Fecha de solicitud firmada por el solicitante)

CONCLUSION:

In the 2018 General Election, over 70% of the people who voted did so during early voting.
(Senate results: Early = 5,994,140 Election Day = 2,340,081 Total votes = 8,334,221)
Under the current laws, there is not a good defense measure in place to reject a voted Limited Ballot.
The Early Ballot Board (EBB) meets after Early Voting is complete. Because the illegal ballot is mixed in with several others all presumed to be valid, the EBB has no way to reject a single ballot.

EFFECTIVE RISK MANAGEMENT AND COUNTERMEASURES:

- Limited Ballot numbers reported to the Secretary of State and posted on their website daily as a separate line item by county. Creating a safeguard to evaluate trends, political parties, candidates or issue groups would have time for analytics to detect abnormalities.
- Require all Limited Ballots to be cast the same as provisional.
- Real-time updates in Texas Election Administration Management (TEAM), to verify the same ID has not been accepted more than once.
- TEAM application should highlight the races a limited voter is allowed to participate in and provide guidance for the election clerk.
- Unique colored marker for the Judge to void out races the limited ballot voter is not partaking in.
- Advisories should have a plain language summary. Confusion arose when it came to the 294th Judicial District showing up in the district chart (PDF) when this district is within Van Zandt County.
    - A lengthy discussion took place between the Election Judge, Clerks and others (no voters present), if outside county voters should be allowed to participate in the 294th race because it was listed in the district chart (PDF) when the district clerk race was not. Two days later this was resolved.

AUTHOR'S BIO:

Lance Lenz is a Certified Information Systems Security Professional (CISSP), granted by the International Information System Security Certification Consortium, also known as (ISC)².
Certified Ethical Hacker (CEH), granted by The International Council of Electronic Commerce Consultants (EC-Council).
Van Zandt County Republican Chairman since 1994, elected every two (2) years by the voters.
Republican Primary official and from 2007 the Ballot Board Judge. Mr. Lenz ran for Texas House in 1992 and 1994 when he came across, firsthand, election fraud from Insider Threat, the block-voting of nursing home residents. This started his drive to understand the inner workings of elections and where the integrity of an election could be compromised.

Signature: 4974277320676F6F6420746F2062652074686520 4B696E67

Thanks to the models "Shar-key" and "Bethinator".

DEFINITIONS:

A threat actor or malicious actor: A person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity. Most often, the term is used to describe the individuals and groups that perform malicious acts against organizations of various types and sizes. From a threat intelligence perspective, threat actors are often categorized as unintentional or intentional and external or internal. *[TechTarget - Threat Actor Definition]*

Security Theater: The practice of investing in countermeasures intended to provide the feeling of improved security while doing little or nothing to achieve it. Benefits of Security Theater are temporary and illusory since after such security measures inevitably fail, not only is the feeling of insecurity increased, but there is also loss of belief in the competence of those responsible for security. *[Schneier, Bruce (2003). Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Copernicus Books. p. 38. ISBN 0-387-02620-7.]*

Social engineering: The art of manipulating people into performing actions or divulging confidential information. *[Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, page 17]*

Research about **Kevin David Mitnick** reveals facts about one of the first of several famous hackers, but he is the one who social engineering is most frequantly linked to.