



How to Backdoor “Invulnerable Code”

Josh Schwartz, Director of Offensive Security @Salesforce

Bio

Offensive Security aka Red Team at Salesforce

"Realistic Adversary Simulation"

"Security Change Catalyst"

I'm a hacker, rule breaker, general troublemaker.



“

“A red team is an independent group that challenges an organization to improve its effectiveness.”

No such thing as "invulnerable code".



At best you get code that is “secure enough”

What is secure enough?

Code without security bugs...?



“

Code that enforces expected states, rather than allowing users to do things with your system that you did not account for.

How do you secure code?

Obvious!?

Don't write code with bugs!

Right?



Yes, you should do that.

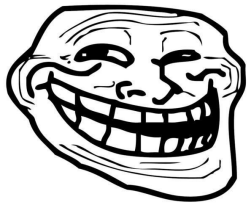
But, there is more...



Let's imagine that "invulnerable code" is this nickel, and on one side is all the lines of code that you write without any security related bugs



Now let's take a look at the other side and flip that nickel over.



problem?

The other side is every other aspect that goes into writing that code.



The third party libraries that you didn't write yourself



The code repo that stores the code



The integration systems that put it together and test it



The build pipeline that moves it around and deploys it



The humans that create and maintain all of those systems



The humans that have access to those human's computers...



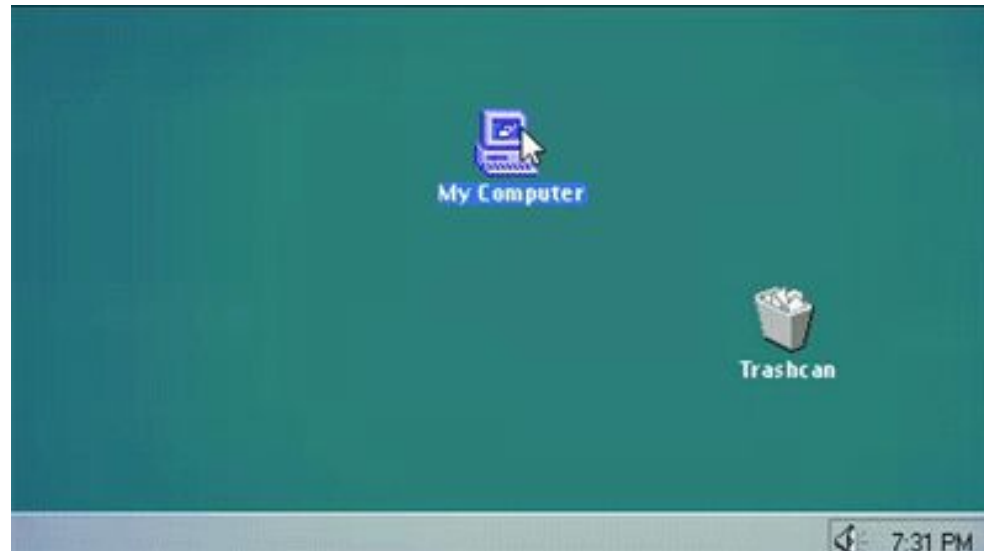
Perhaps some of you realize there is still another side of this coin?



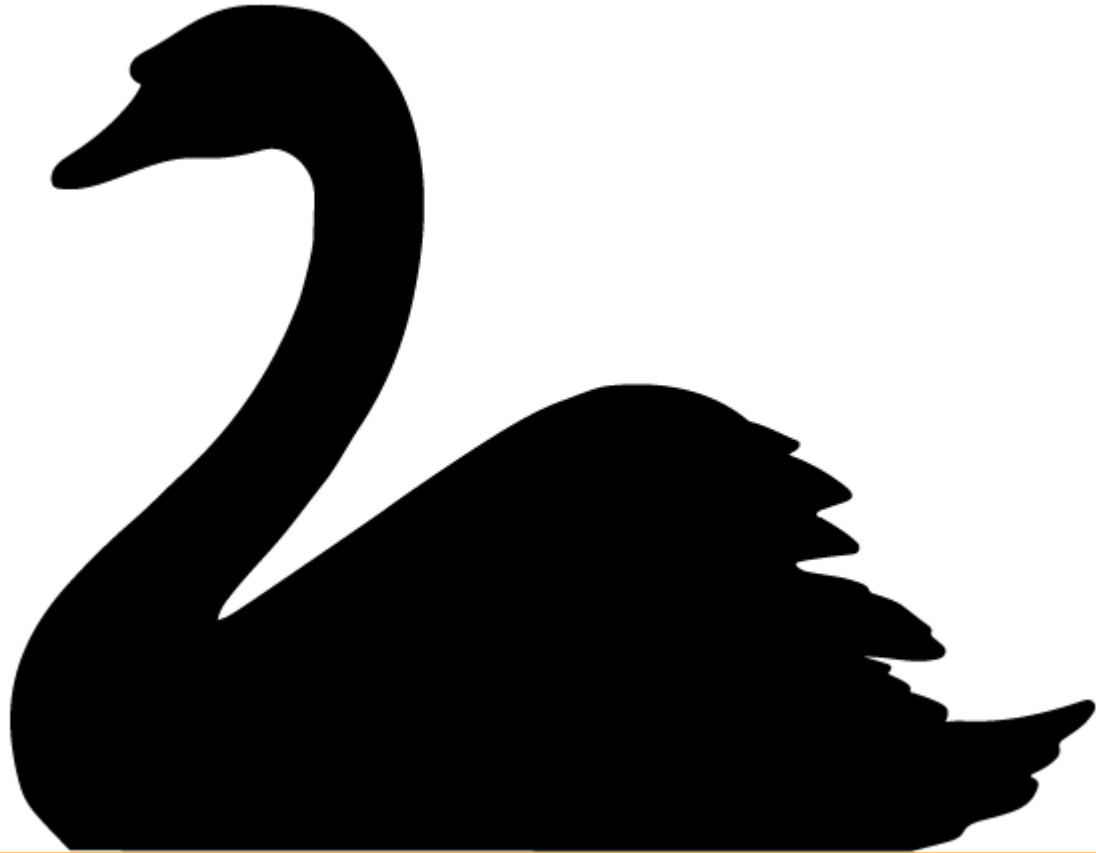
It's the side you don't see.

The side you can't see.

The things we can't account for.



The Black Swan Theory



Accept there is no ubiquitous security perfection



We can think like an adversary

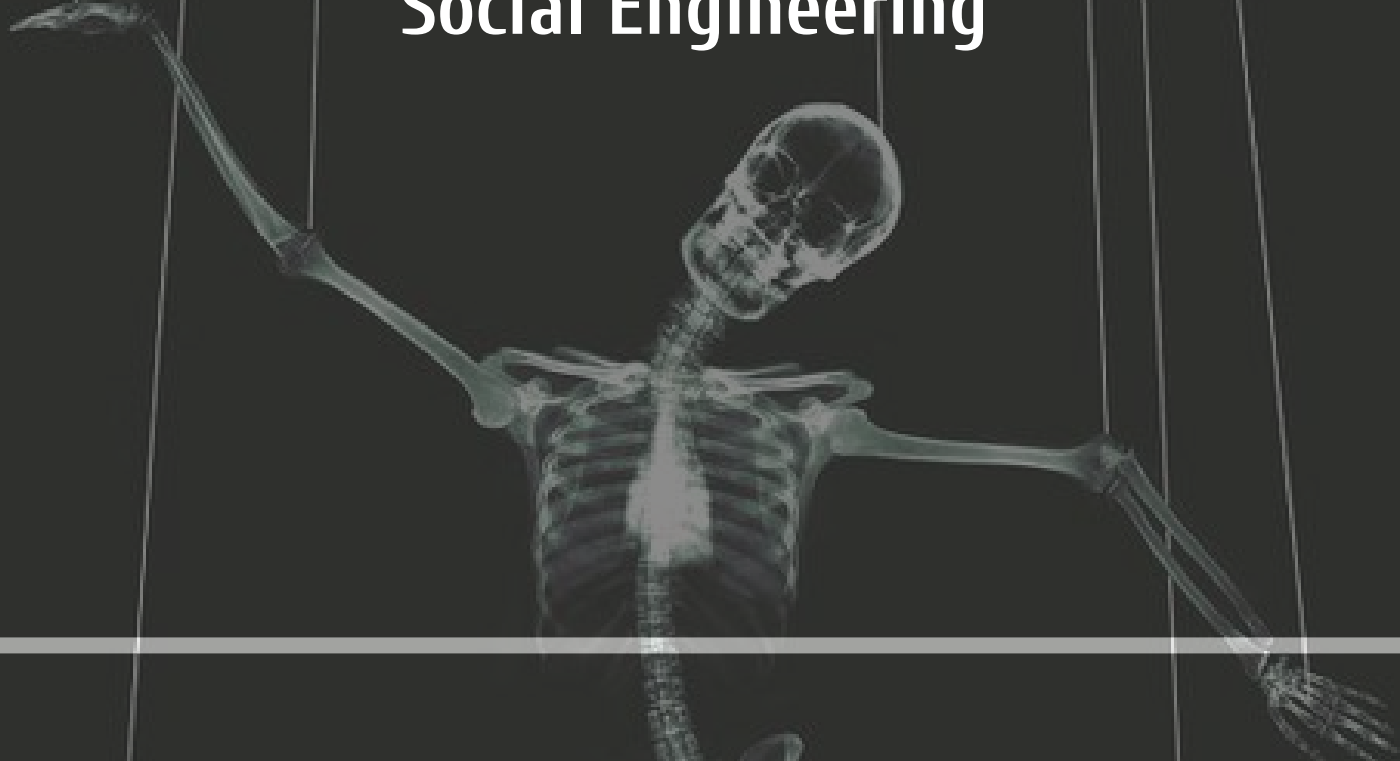
We can challenge where we set the bar



*I'm going to share with you
some of my tactics as the attacker*

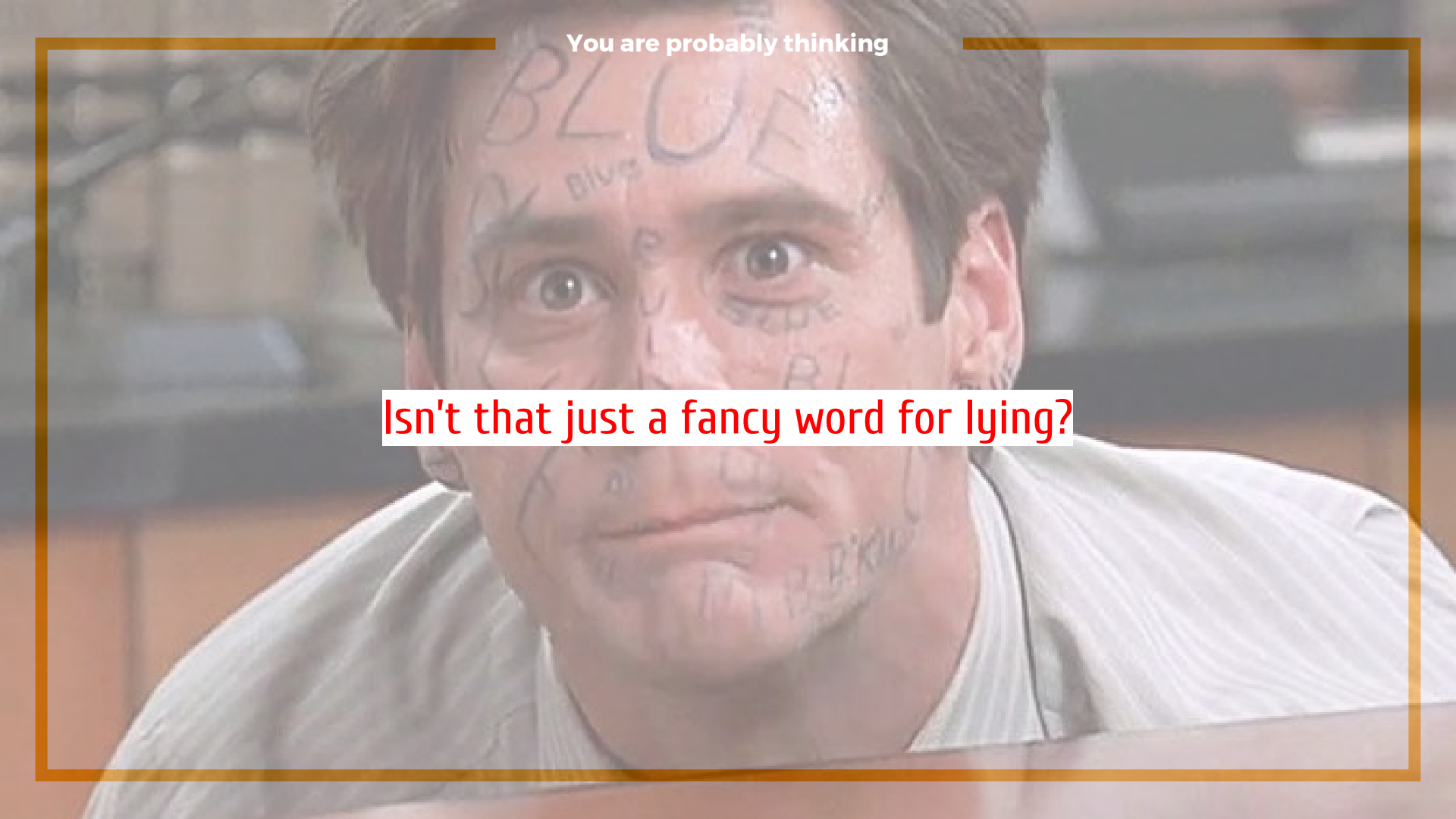
What is

Social Engineering



You are probably thinking

Isn't that just a fancy word for lying?



“

“Any act that influences a person to take an action that may or may not be in their best interest”

Influence through emotional response

Pretext

Manipulation vs Elicitation

Social Engineering vs. Phishing



- ❑ Classic Credential Capturing
- ❑ The Nigerian Prince with a Diamond Mine
- ❑ The IRS Call

This type of phishing is weak.

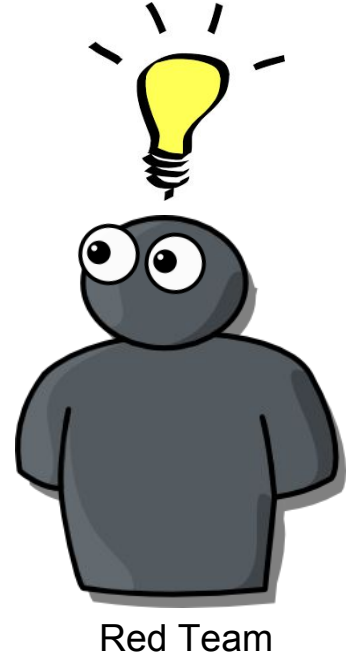
Phishing

It's impersonal.

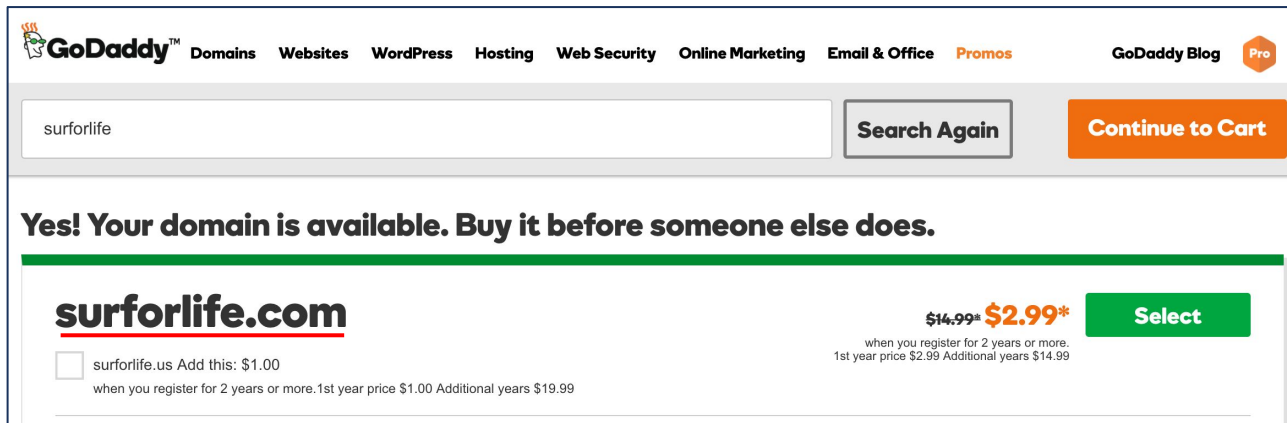
- ❑ More targeted
- ❑ More personal
- ❑ More effort per person
- ❑ Less likely to be detected
- ❑ More likely to succeed



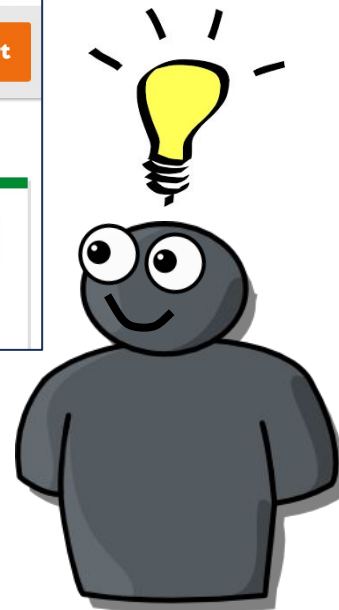
Spear Phishing Example



Spear Phishing Example

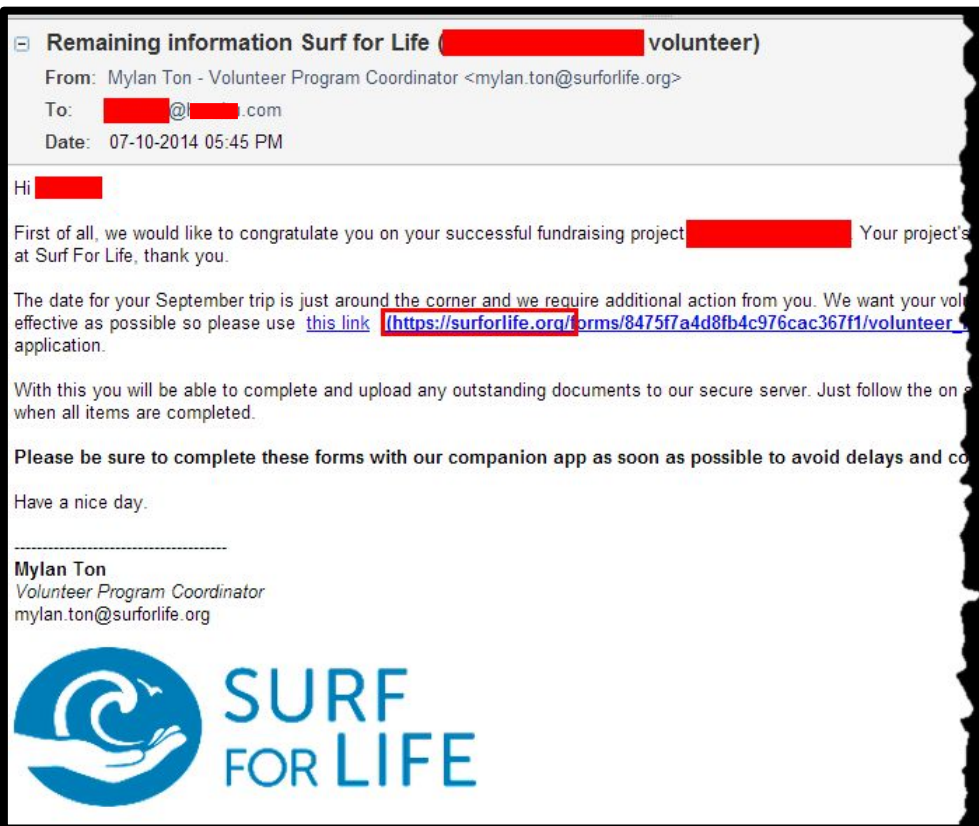


The screenshot shows a GoDaddy search interface. At the top, the GoDaddy logo is followed by navigation links: Domains, Websites, WordPress, Hosting, Web Security, Online Marketing, Email & Office, and Promos. On the right, there are links for 'GoDaddy Blog' and a 'Pro' badge. A search bar contains the text 'surforlife', with a 'Search Again' button to its right and a 'Continue to Cart' button further right. Below the search bar, a green banner reads 'Yes! Your domain is available. Buy it before someone else does.' Underneath, the domain 'surforlife.com' is displayed in a large font with a red underline. To the left of the domain is a checkbox and the text 'surforlife.us Add this: \$1.00 when you register for 2 years or more. 1st year price \$1.00 Additional years \$19.99'. To the right of the domain, the price is shown as '\$14.99*' crossed out and '\$2.99*' in bold, with a 'Select' button. Below the price, smaller text reads 'when you register for 2 years or more. 1st year price \$2.99 Additional years \$14.99'.

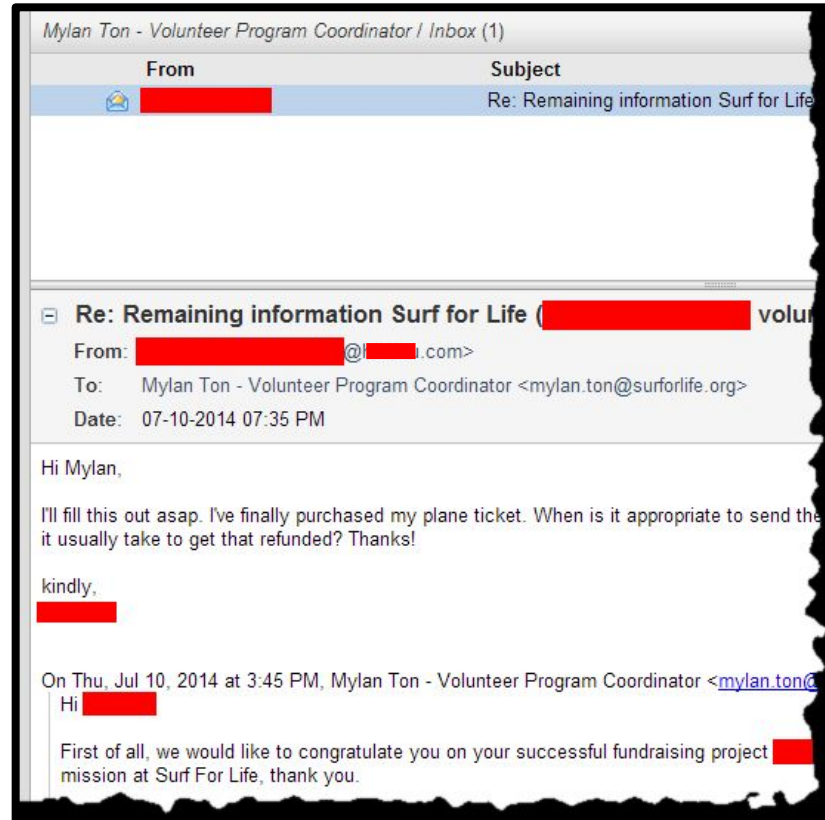


Red Team

Speare Phishing Example



Spear Phishing Example



Spear Phishing Example

Of course there is no form



Spear Phishing Example



Step 1: Social Recon



Social Recon

The screenshot shows a Google search interface. The search bar contains the query "site:linkedin.com -jobs rick and morty". The search results are displayed on page 4 of 683 results. The results list several LinkedIn profiles related to the show "Rick and Morty".

Page 4 of about 683 results (0.56 seconds)

Beth Goldsby profiles | LinkedIn
www.linkedin.com/pub/dir/Beth/Goldsby
Title: Assistant to Justin Roiland at **Rick and Morty**; Demographic info: Greater Los Angeles Area | Entertainment. Current: Assistant to Justin Roiland at **Rick and** ...

Jim Mcdermott - Greater Los Angeles Area profiles | LinkedIn
www.linkedin.com/pub/dir/Jim/.../us-49-Greater-Los-Angeles-Area ▾
I have created and art directed a few pilots for FOX, Adult Swim, and Spike. I am currently art directing "**Rick and Morty**", a new animated show for Adult Swim, ...

Naegele - Greater Los Angeles Area - LinkedIn
www.linkedin.com/pub/dir/+Naegele/us-49-Greater-Los-Angeles-Area
Current: Associate Producer for **Rick and Morty** at Starburns Industries (Sole Proprietorship); Past: Production Coordinator for **Rick and Morty** - Season 1 at ...

Jon Vermilyea | LinkedIn
www.linkedin.com/in/jonvermilyea
Greater Los Angeles Area - Storyboard Revisionist at Cartoon Network Starburns Industries. Sole Proprietorship; 51-200 employees; Entertainment industry. 2012 - 2012 (less than a year) Burbank, CA. **Rick and Morty** Pilot ...

Scott Alberts | LinkedIn
www.linkedin.com/pub/scott-alberts/0/34/248 ▾
Des Moines, Iowa Area. Scott Alberts, Storyboard Artist ("**Rick and Morty**") at Starburns Industries. Barcelona Area, Spain. K. Scott Alberts,. Columbia, Missouri ...



Brent Noll

Prop and Effect Designer at Rick And Morty

Covina, California | Entertainment

Previous NBC - Community, Planet Phamus, Harmon Quest

Education Texas State University-San Marcos

Send Brent InMail



91
connections



Websites

[BrentNoll.com](#)

[Company Website](#)

[Blog](#)



Contact Info



www.linkedin.com/in/brentnoll



Experience

Prop and Effect Designer

Rick And Morty

May 2014 – Present (6 months) | Burbank

Designing Props/ Effects for Season 2 of Rick and Morty,

Working under Art Director James McDermott and Director Pete Michels to design props, sci fi gadgets, ships, vehicles and other visual effects for Adult swims Prime time Comedy Rick and Morty

Rick and Morty an animated series for Adult Swim created by Dan Harmon and Justin Roiland, and produced at Starburns Industries.



Watch Full Episodes of Rick and Morty Now on AdultSwim.com



BRENT TUMBLES

Im Brent Noll. I draw Cartoons. Drink Coffee and etc.

I am an animation illustrator and designer for television, I have worked on Rick and Morty, And G.I. Jeff (Community NBC) as well as other Starburns related projects

[MY MAIN SITE](#)

[ABOUT ME](#)

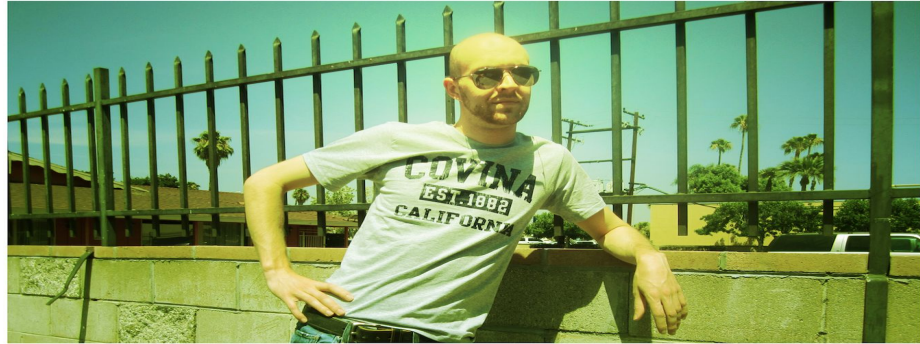
[HIRE ME](#)

[STORE](#)

[ANSWER ME THIS BUDDY](#)

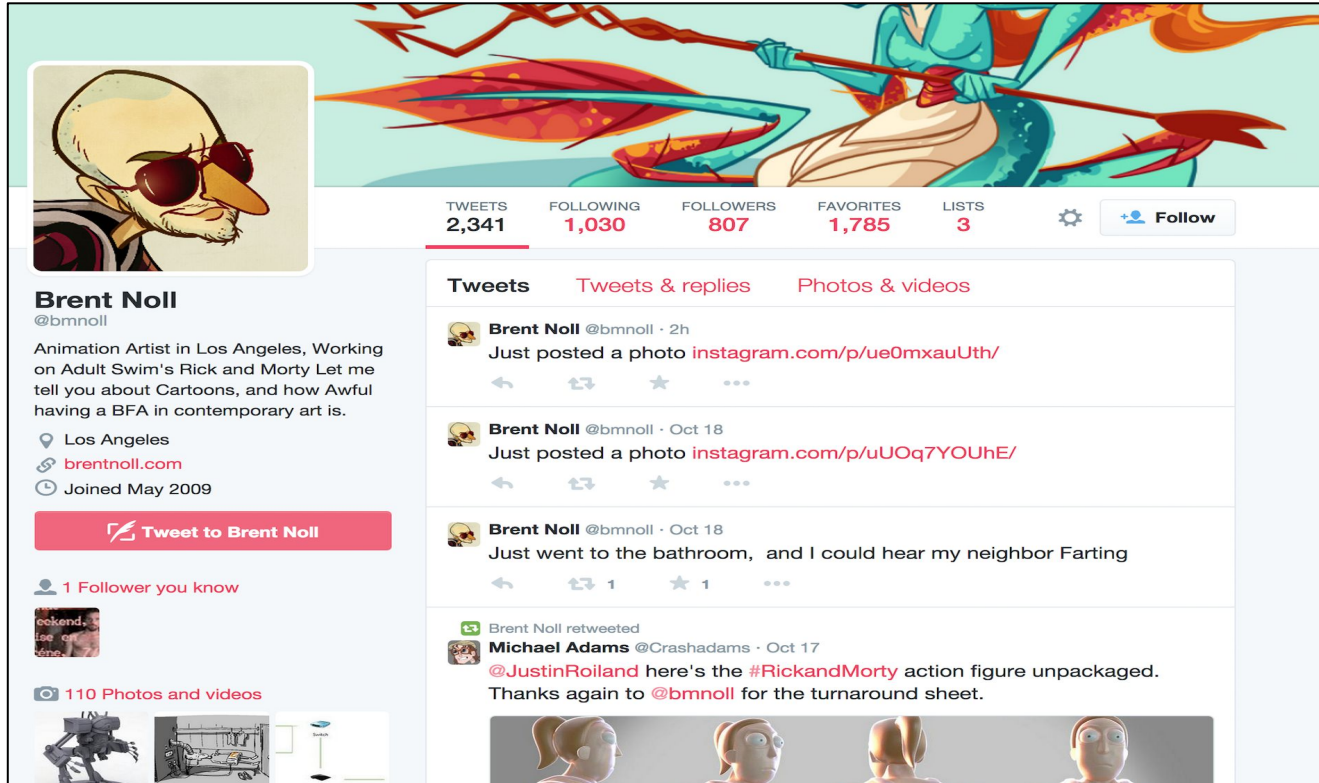


ABOUT ME



*Hello, My name is Brent, Im 25 and i like to draw cartoons. I am an Animation Illustrator and Designer. I currently work at **Starburns Industries**, As well as Freelance Illustration. Feel free to send me a message anytime if you have questions about drawing, cartoons, or if you just want to say Hi.*

Social Recon: Twitter



The image shows a screenshot of a Twitter profile for Brent Noll (@bmnoll). The profile picture is a cartoon illustration of a man with a large nose and sunglasses. The header features a colorful illustration of a character in a boat. The profile information includes the name 'Brent Noll', handle '@bmnoll', location 'Los Angeles', website 'brentnoll.com', and 'Joined May 2009'. There is a 'Tweet to Brent Noll' button and a list of 1 follower. The tweet history shows three tweets: two about Instagram posts and one about a bathroom incident. A retweet by Michael Adams is also visible, mentioning Justin Roiland and Rick and Morty. At the bottom, there are thumbnails for photos and videos, including a robot and a hospital bed.

TWEETS 2,341 **FOLLOWING** 1,030 **FOLLOWERS** 807 **FAVORITES** 1,785 **LISTS** 3

Brent Noll
@bmnoll

Animation Artist in Los Angeles. Working on Adult Swim's Rick and Morty Let me tell you about Cartoons, and how Awful having a BFA in contemporary art is.

Los Angeles
brentnoll.com
Joined May 2009

1 Follower you know

110 Photos and videos

Tweets Tweets & replies Photos & videos

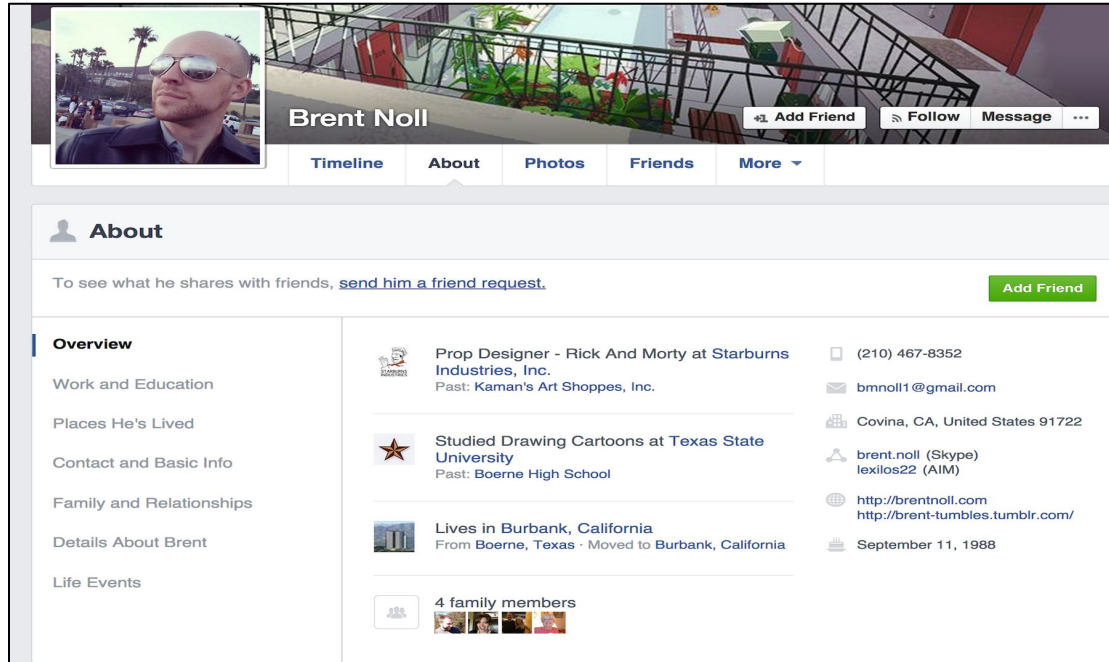
Brent Noll @bmnoll · 2h
Just posted a photo [instagram.com/p/ue0mxauUth/](https://www.instagram.com/p/ue0mxauUth/)

Brent Noll @bmnoll · Oct 18
Just posted a photo [instagram.com/p/uUOq7YOUhE/](https://www.instagram.com/p/uUOq7YOUhE/)

Brent Noll @bmnoll · Oct 18
Just went to the bathroom, and I could hear my neighbor Farting

Brent Noll retweeted
Michael Adams @Crashadams · Oct 17
[@JustinRoiland](#) here's the [#RickandMorty](#) action figure unpackaged. Thanks again to [@bmnoll](#) for the turnaround sheet.

Social Recon: Facebook



The image shows a screenshot of a Facebook profile page for Brent Noll. The profile picture is a man with sunglasses. The cover photo is a 3D architectural rendering of a modern building with a balcony. The name 'Brent Noll' is displayed prominently. Below the name are navigation tabs for 'Timeline', 'About', 'Photos', 'Friends', and 'More'. The 'About' section is expanded, showing a sidebar with categories like 'Overview', 'Work and Education', 'Places He's Lived', 'Contact and Basic Info', 'Family and Relationships', 'Details About Brent', and 'Life Events'. The main content area of the 'About' section lists his current job as a Prop Designer at Starburns Industries, Inc., his education at Texas State University, his current residence in Burbank, California, and his birth date of September 11, 1988. It also shows contact information for phone, email, and social media links, as well as a list of 4 family members.

Brent Noll [Add Friend](#) [Follow](#) [Message](#) ...


[Timeline](#) [About](#) [Photos](#) [Friends](#) [More](#) ▾


About


To see what he shares with friends, [send him a friend request](#). [Add Friend](#)


Overview


- Work and Education
- Places He's Lived
- Contact and Basic Info
- Family and Relationships
- Details About Brent
- Life Events


 **Prop Designer - Rick And Morty at Starburns Industries, Inc.**
Past: Kaman's Art Shoppes, Inc.


 **Studied Drawing Cartoons at Texas State University**
Past: Boerne High School


 **Lives in Burbank, California**
From Boerne, Texas - Moved to Burbank, California


 (210) 467-8352


 bmnoll1@gmail.com


 Covina, CA, United States 91722

 [brent.noll \(Skype\)](#)
[lexilos22 \(AIM\)](#)

 <http://brentnoll.com>
<http://brent-tumbles.tumblr.com/>

 September 11, 1988

 **4 family members**



Social Recon: Google Sites

The image shows a screenshot of a Google+ profile page for Brent Noll. The browser's address bar displays the URL <https://plus.google.com/+BrentNoll/about>. The Google+ logo and search bar are visible at the top. The profile header includes a circular profile picture of a cartoon character with sunglasses, the name "Brent Noll", and biographical information: "Works at Starburns Industries", "Attended Texas State", and "Lives in Covina, CA 91722, United States". A red "Add to circles" button is present, along with statistics for "1,546 followers | 26,491 views". The main cover image is a large, colorful cartoon illustration of a character on a motorcycle. Below the header, navigation tabs for "About", "Posts", "Photos", and "YouTube" are shown. The "About" section is expanded, showing a "People" subsection with "In his circles" listing "Charlie Roch" with an "Add" button, and a "Story" subsection with a "Tagline" that reads "I'm Brent Noll. I draw Cartoons. Drink Coffee and etc." and an "Introduction" section.

Brent Noll

Works at Starburns Industries
Attended Texas State
Lives in Covina, CA 91722, United States

+ Add to circles

1,546 followers | 26,491 views

About Posts Photos YouTube

People

In his circles 1,477 people

Charlie Roch + Add

Story

Tagline
I'm Brent Noll. I draw Cartoons. Drink Coffee and etc.

Introduction

Brent Noll



linkedin: <https://www.linkedin.com/in/brentnoll>

twitter: <https://twitter.com/bmnoll>

tumblr: <http://brent-tumbles.tumblr.com/>

facebook: <https://www.linkedin.com/in/brentnoll>

instagram: <http://instagram.com/bmnoll1>

website: <http://brentnoll.com/>

youtube: <https://www.youtube.com/channel/UC9pSlpwgYdBwdwCoH1ZDG8Q>

google+: <https://plus.google.com/+BrentNoll/>

location: Covina, CA, United States 91722

phone number: (210) 467-8352

skype: brent.noll

aim: [lexilos22](#)

email: bmnoll1@gmail.com

notes: draws props for rick and morty. really active on social media.

Attackers can stalk you using the internet to get access to the things that you have access to. This is not a new thing.

also it get's worse.

Identity Duplication: Orig

The image shows a screenshot of a Google+ profile page for Brent Noll. The browser's address bar displays the URL <https://plus.google.com/+BrentNoll/about>. The profile header includes a circular profile picture of a cartoon character with sunglasses, the name "Brent Noll", and biographical information: "Works at Starburns Industries", "Attended Texas State", and "Lives in Covina, CA 91722, United States". There is a red "Add to circles" button and statistics showing "1,546 followers | 26,491 views". The main cover image is a large, vibrant cartoon illustration of a character on a motorcycle against a sunset background. Below the cover are navigation tabs for "About", "Posts", "Photos", and "YouTube". The "About" section is expanded, showing a "People" section with "In his circles" (1,477 people) and a list of people, including Charlie Roch with an "Add" button. A "Story" section is also visible, containing a "Tagline" and an "Introduction".

Brent Noll

Works at Starburns Industries
Attended Texas State
Lives in Covina, CA 91722, United States

+ Add to circles

1,546 followers | 26,491 views

About Posts Photos YouTube

People

In his circles 1,477 people

Charlie Roch + Add

Story

Tagline
I'm Brent Noll. I draw Cartoons. Drink Coffee and etc.

Introduction

Identity Duplication: Fake

The image shows a screenshot of a Google+ profile page for Brent Noll. The browser's address bar shows the URL: <https://plus.google.com/u/0/117138238194473799029...>. The profile header includes a profile picture of a character with sunglasses, the name "Brent Noll", and the text: "Works at Starburns Industries", "Attended Texas State", and "Lives in Covina, CA 91722, United States". There is a red "Add to circles" button. The cover image is a cartoon illustration of a character on a motorcycle with a gun, set against a sunset background. Below the cover image are tabs for "About", "Posts", "Photos", and "Videos". The "About" section is expanded, showing a "Story" section with a "Tagline" that reads "I'm Brent Noll. I draw Cartoons. Drink Coffee and etc." and an "Introduction" that reads "to draw cartoons.". The "Work" section lists "Occupation" as "Free lance Illustration for Animation" and "Skills" as "Character Bg and Prop Design/ Color key Photoshop, Illustrator, Indesign, After Effects, Flash".

Brent Noll

Works at Starburns Industries
Attended Texas State
Lives in Covina, CA 91722, United States

+ Add to circles

About Posts Photos Videos

Story

Tagline
I'm Brent Noll. I draw Cartoons. Drink Coffee and etc.

Introduction
to draw cartoons.

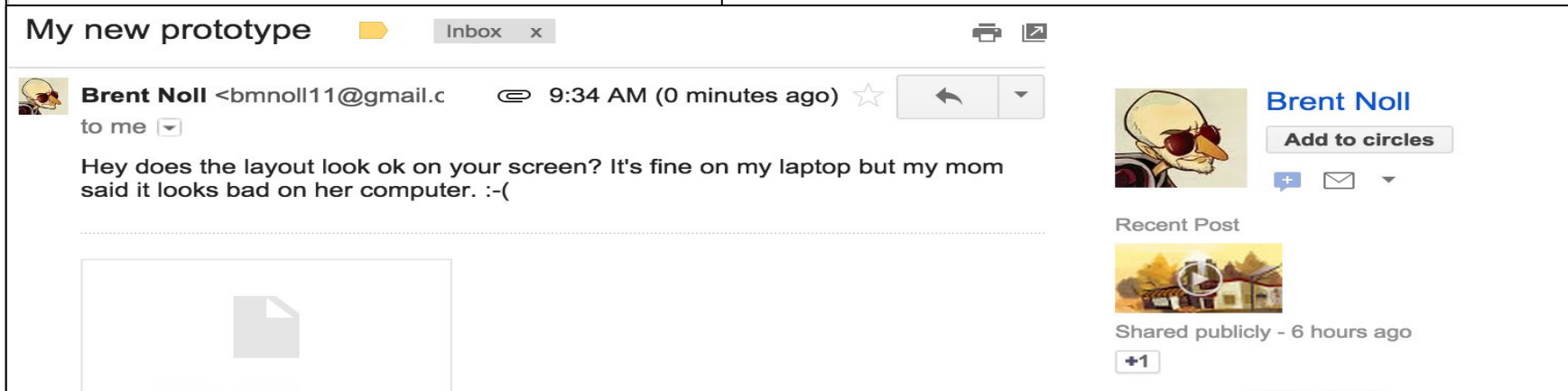
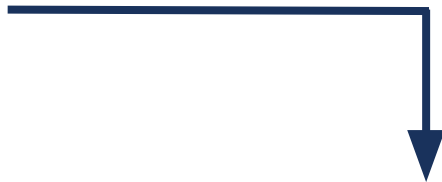
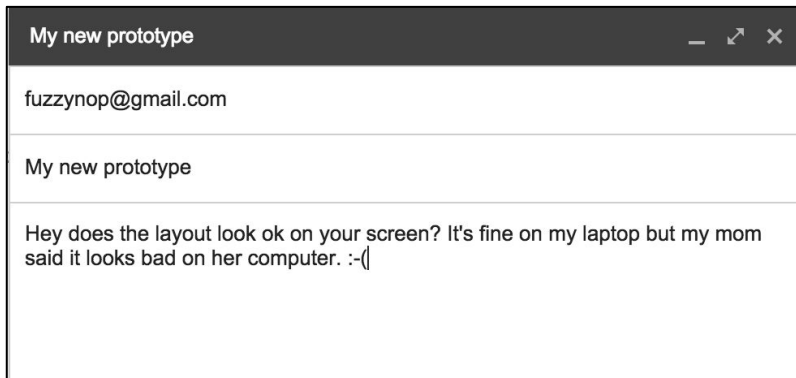
Work

Occupation
Free lance Illustration for Animation

Skills
Character Bg and Prop Design/ Color key Photoshop,
Illustrator, Indesign, After Effects, Flash

Cloning public profiles allows a social engineer to leverage a targets subliminal familiarity with identity based content to gain instant rapport.

Identity Duplication: Result



Blocking malicious file types in emails

As a security measure to prevent potential viruses, Gmail doesn't allow you to send or receive executable files (such as files ending in .exe). Executable files can contain harmful code that might cause malicious software to download to your computer. In addition, Gmail doesn't allow you to send or receive corrupted files, files that don't work properly.



File types that can't be sent or received

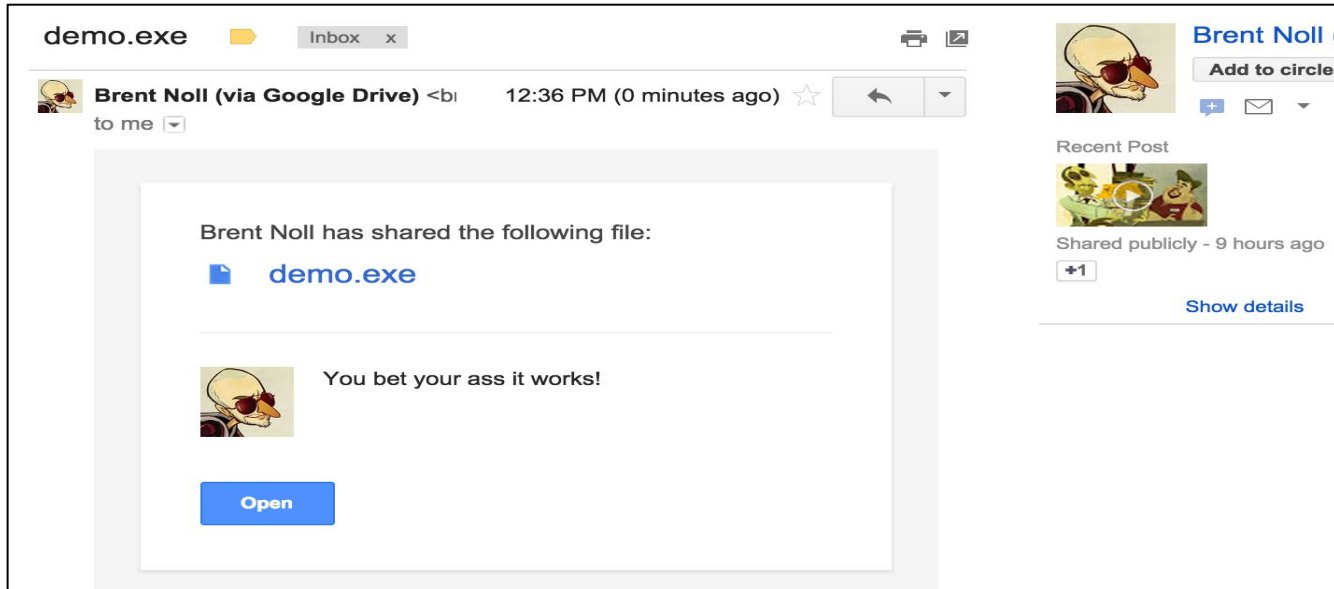
You can't send or receive the following file types:

```
.ade, .adp, .bat, .chm, .cmd, .com, .cpl, .exe, .hta, .ins, .isp, .jse, .lib,  
.lnk, .mde, .msc, .msp, .mst, .pif, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vxd,  
.wsc, .wsf, .wsh
```

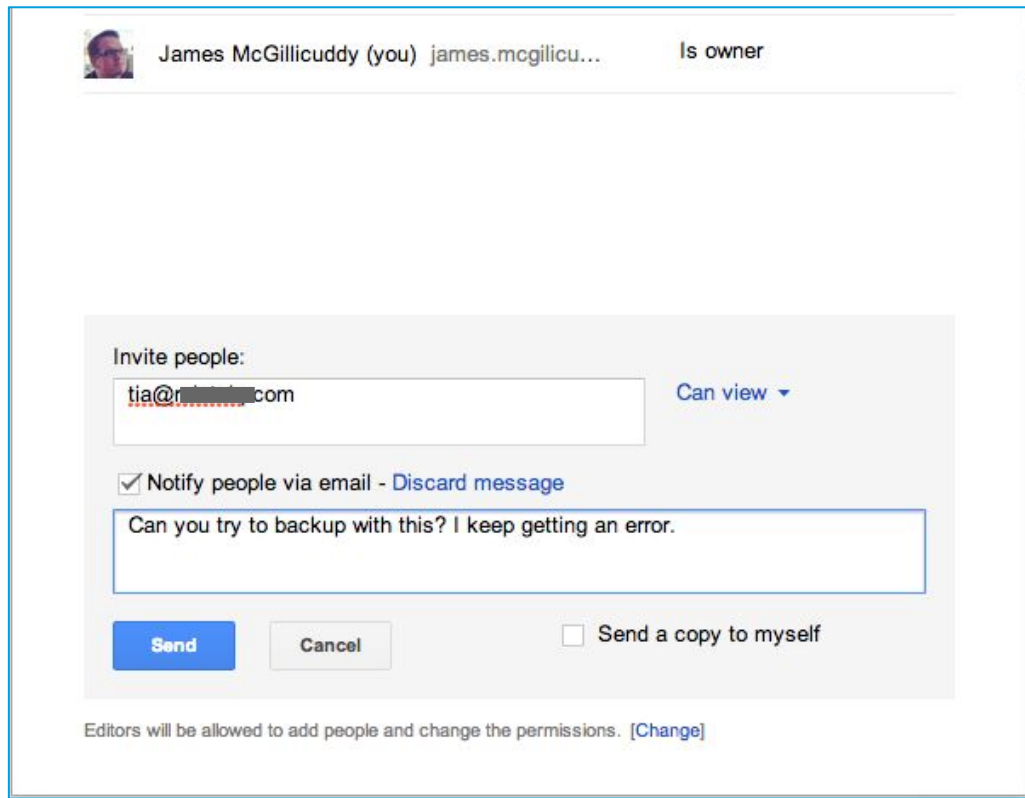
Messages containing the types of files listed above will be bounced back and returned to the sender automatically. Gmail won't accept these file types even if they're sent in a zipped format. Here are some examples of zipped formats:

```
.zip, .tar, .tgz, .taz, .z, .gz, .rar
```

You can share any type of file through Google Drive



Real Example



The screenshot shows the sharing settings for a document. At the top, the owner is identified as James McGillicuddy (you) with the email james.mcgilicu... and the role 'Is owner'. Below this is a section for inviting people. The 'Invite people:' label is followed by a text input field containing 'tia@redacted.com' and a dropdown menu set to 'Can view'. A checkbox for 'Notify people via email' is checked, with a link to 'Discard message'. A text area contains the message: 'Can you try to backup with this? I keep getting an error.'. At the bottom of the invite section are 'Send' and 'Cancel' buttons, and a checkbox for 'Send a copy to myself' which is unchecked. Below the invite section, a note states: 'Editors will be allowed to add people and change the permissions. [Change]'.

James McGillicuddy (you) james.mcgilicu... Is owner

Invite people:

tia@redacted.com Can view ▾

Notify people via email - [Discard message](#)

Can you try to backup with this? I keep getting an error.

Send Cancel Send a copy to myself

Editors will be allowed to add people and change the permissions. [\[Change\]](#)

They receive this

On Mon, Sep 8, 2014 at 1:42 PM, James McGillicuddy (via Google Drive) <james.mcgillicuddy@gmail.com> wrote:


I've shared an item with you.


can you check real quick if this will open for you?

 [backup_relationships.jar](#)

Google Hosts the file



Apologies.
There is no preview available.

 Download

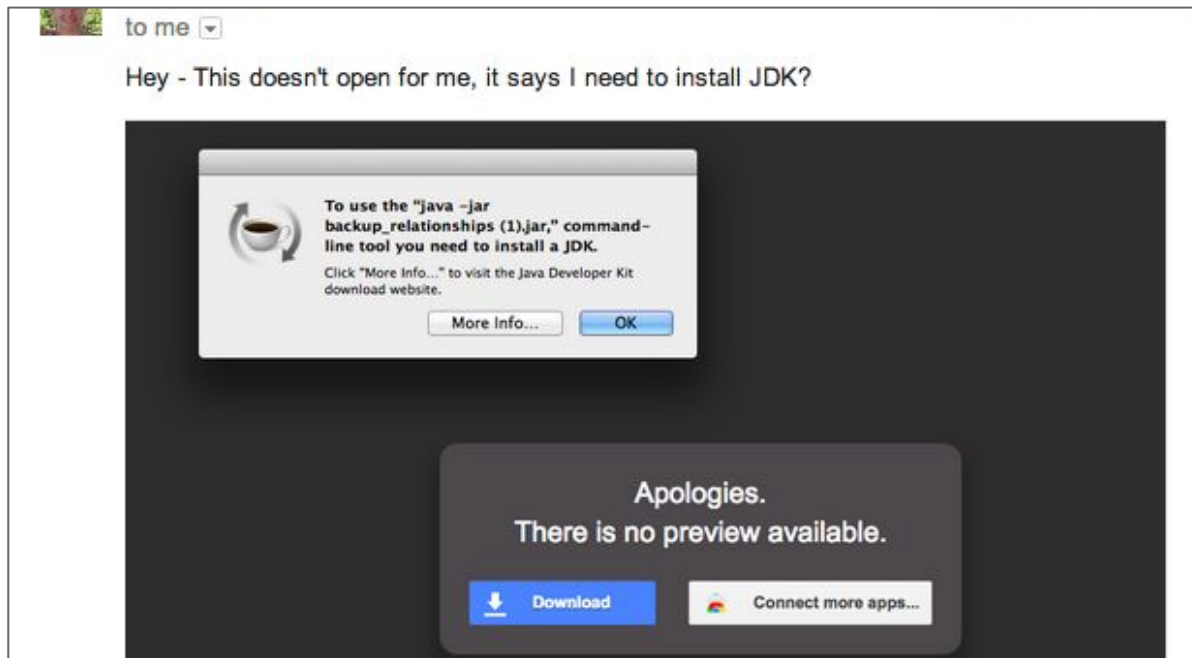
 Connect more apps...

Try one of the apps below to open or edit this item

Suggested third-party apps

-  ZIP Extractor
-  CloudConvert

They send back:





But




What if something so simple doesn't work?


Example 2

1. Notice our target has nice offices from pictures they post on social media
2. Create our pretext:
Freelance journalist for a magazine that features interior design
3. Contact target asking to feature them alongside other big companies
4. Set up "interview"

Our request gets a response and fwd from their PR firm

Intro to Anthony Taylor at LifeEdited.com Inbox x  

 **Mary [REDACTED]** <[REDACTED]@pr.com> 11:43 AM (4 minutes ago) ☆  

to Katie, [REDACTED] 

Hi Katie,

By way of this email, I am connecting you with Anthony Taylor at LifeEdited to help set up an interview and tour at [REDACTED]. As we discussed, LifeEdited will be featuring office spaces that have interesting interior design and culture that foster creativity. They will be featuring the office spaces of big companies like FaceBook and Twitter and would also like to feature [REDACTED] office space in this piece slated to run October 20th.

I'll let you take it from here.

Best,
Mary

Example 2

They are totally stoked and set up the interview



Katie [redacted] <katie@[redacted].com>

1:04 PM (16 minutes ago) ☆



to me, [redacted], Mary ▾

Thank you, Mary!

Anthony, it's a pleasure to meet you. I understand you'd like to come by and tour our offices. Are you available Wednesday, September 24, between 10 and 3? Please let me know how long you think you'll need and I'll schedule out the visit with our head of operations, Stephen [redacted]

Thanks,
Katie



Example 2

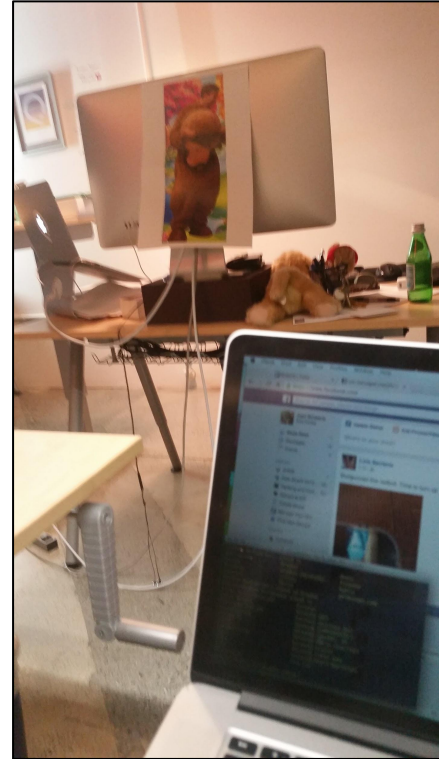
- Interview and tour of offices lasts for about 4 hours
- Take pictures of security systems, whiteboards, post-it notes, etc.
- Spring the trap

Example 2



Permission for Photography of Property

For good and valuable consideration herein acknowledged as received, the undersigned, being the legal owner of, or having the right to permit the taking and use of photographs of, certain property designated as ~~Redacted address~~ located at ~~300 S. Embarcadero Street~~ Palo Alto, CA 94301, does irrevocably grant to LifeEdited.com and assigns the full perpetual rights to take and use such photographs in publications both digital and print. The undersigned hereby warrants that he/she is a legally competent adult and has every right to contract in his/her own name in the above regard. The undersigned states further that he/she has read the above authorization, release, and agreement, prior to its execution, and that he/she is fully familiar with the contents thereof. If the undersigned is signing as an agent or employee of a firm or corporation, the undersigned warrants that he/she is fully authorized to do so. This release shall be binding upon the undersigned and his/her/its heirs, legal representatives, successors, and assigns.



Example 2



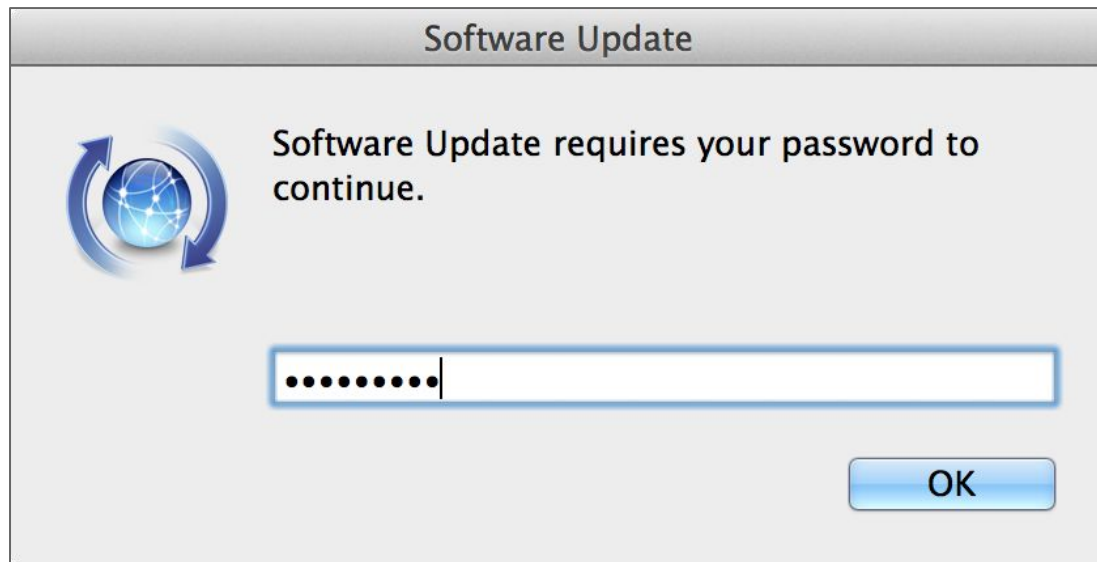
What then?

So what happens after you get that access?

Sure would be nice to get that person's password...

Local Phishing

```
osascript -e 'tell app "System Events" to display dialog "Software Update requires your password to apply ." & return & return default answer "" with icon file ":System:Library:CoreServices:Software Update.app:Contents:Resources:SoftwareUpdate.icns" with hidden answer with title "Software Update" buttons {"OK"} default button "OK"'
```



Local Phishing

```
$credential = $host.ui.PromptForCredential("Credentials Required", "Please enter your user name and password.",  
"$env:username", "NetBiosUserName")
```

```
$credential.Password | ConvertFrom-SecureString
```

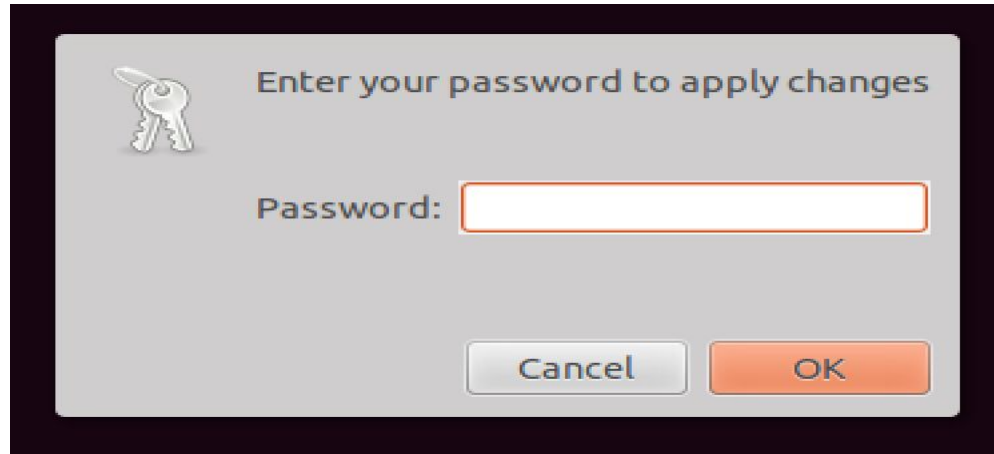
```
$env:username
```

```
$credential.GetNetworkCredential().password
```



Local Phishing

```
DISPLAY=:0 gksudo -p -m "Enter your password to apply changes."
```



We are good at stealing passwords.

2FA will go a long way here.

It makes it way harder for us but it isn't perfect.

Here are a few ways we get around it:

Cookie Stealing



Bypassing 2FA



Continuous Integration



you understand the company

you have access internally

you have passwords

you can bypass 2FA

you have access to internal documents

you have access to servers

you have access to the code pipeline

Is backdooring your production code really that hard?

Zero Bugs



This isn't everything



The End



@AARONSANIMALS

Questions / Complaints?



Thank You

