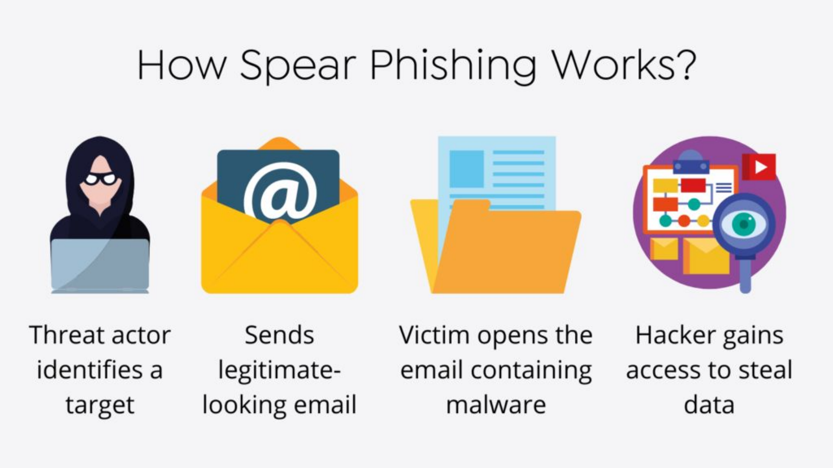
Operation Ahab

•••

Talen Flippo | George Kell | Tristan Khim | Brandon O’Leary | Rodney Ramirez

Cohort 2206

Intro



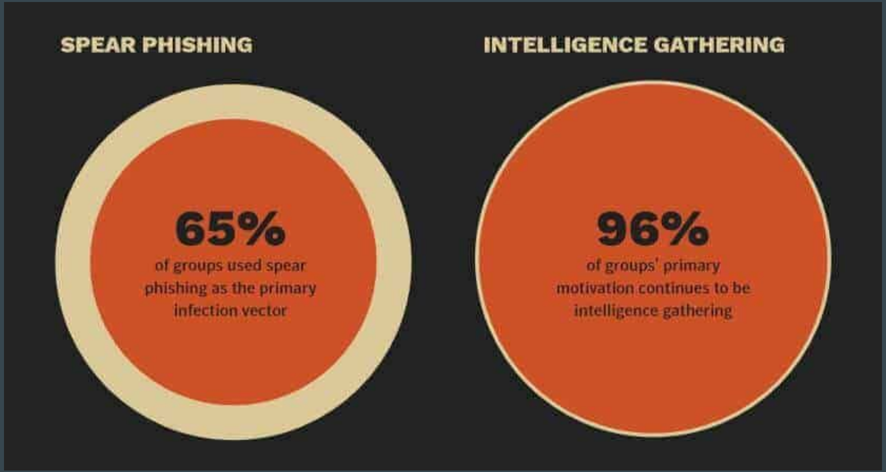
How Spear Phishing Works?

Threat actor identifies a target

Sends legitimate-looking email

Victim opens the email containing malware

Hacker gains access to steal data



SPEAR PHISHING

65% of groups used spear phishing as the primary infection vector

INTELLIGENCE GATHERING

96% of groups' primary motivation continues to be intelligence gathering

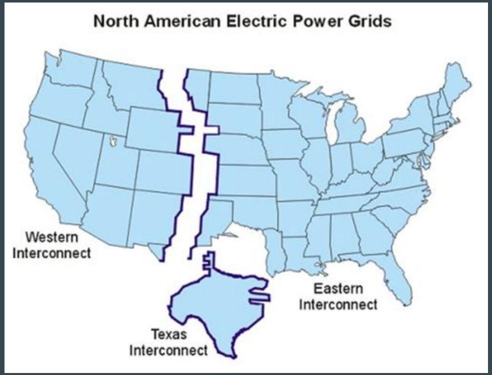
Spear Phishing

Some of the biggest companies to fall to phishing attacks are:

- JPMorgan Chase
- Sony Pictures
- The US Power Grid

J.P.Morgan

SONY PICTURES

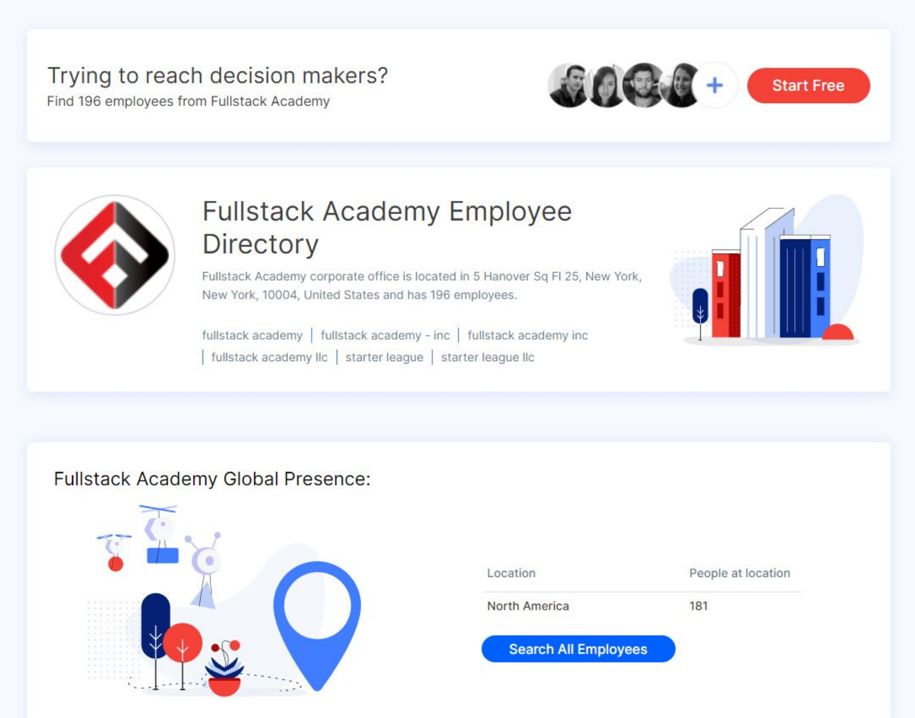

North American Electric Power Grids

Target & Gameplan

- Recon
- Email Phishing Creation
- Faux Website Development
- Payload Creation & Execution

Recon

- Search Fullstack Academy employees
- Directory with +400 employees



Trying to reach decision makers?

Find 196 employees from Fullstack Academy

Fullstack Academy Employee Directory

Fullstack Academy corporate office is located in 5 Hanover Sq Fl 25, New York, New York, 10004, United States and has 196 employees.

fullstack academy | fullstack academy - inc | fullstack academy inc | fullstack academy llc | starter league | starter league llc

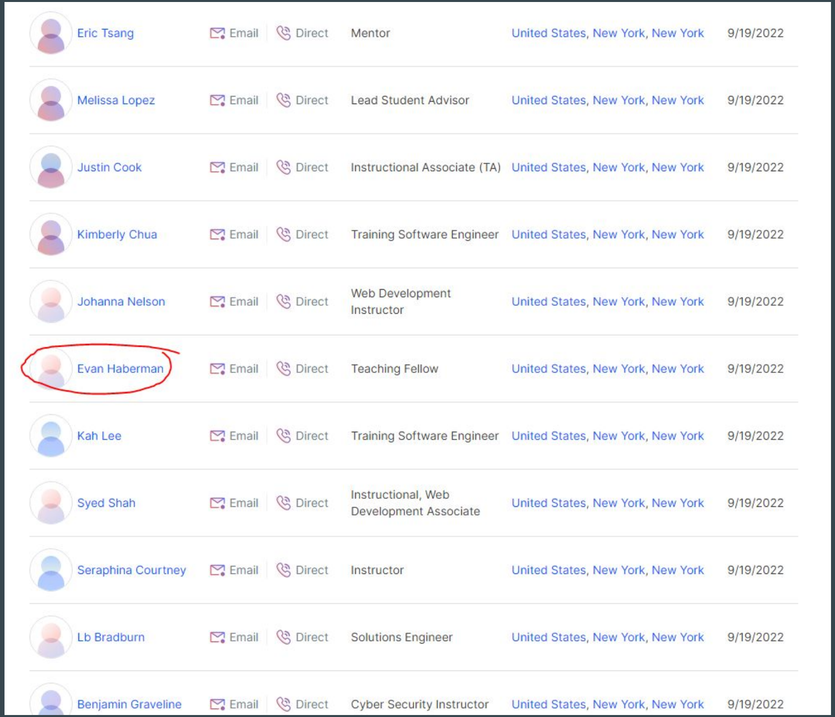
Fullstack Academy Global Presence:

Location	People at location
North America	181

Recon

Here we found Evan Haberman

Next we are going to specifically look up his name and see what we can find.



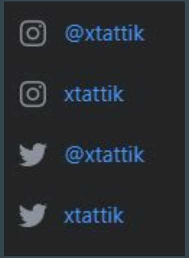
Eric Tsang	Email	Direct	Mentor	United States, New York, New York	9/19/2022
Melissa Lopez	Email	Direct	Lead Student Advisor	United States, New York, New York	9/19/2022
Justin Cook	Email	Direct	Instructional Associate (TA)	United States, New York, New York	9/19/2022
Kimberly Chua	Email	Direct	Training Software Engineer	United States, New York, New York	9/19/2022
Johanna Nelson	Email	Direct	Web Development Instructor	United States, New York, New York	9/19/2022
Evan Haberman	Email	Direct	Teaching Fellow	United States, New York, New York	9/19/2022
Kah Lee	Email	Direct	Training Software Engineer	United States, New York, New York	9/19/2022
Syed Shah	Email	Direct	Instructional, Web Development Associate	United States, New York, New York	9/19/2022
Seraphina Courtney	Email	Direct	Instructor	United States, New York, New York	9/19/2022
Lb Bradburn	Email	Direct	Solutions Engineer	United States, New York, New York	9/19/2022
Benjamin Graveline	Email	Direct	Cyber Security Instructor	United States, New York, New York	9/19/2022

Recon

Found him on Facebook!

Looks like he's linked his other social media accounts to his bio

Let's take a look...

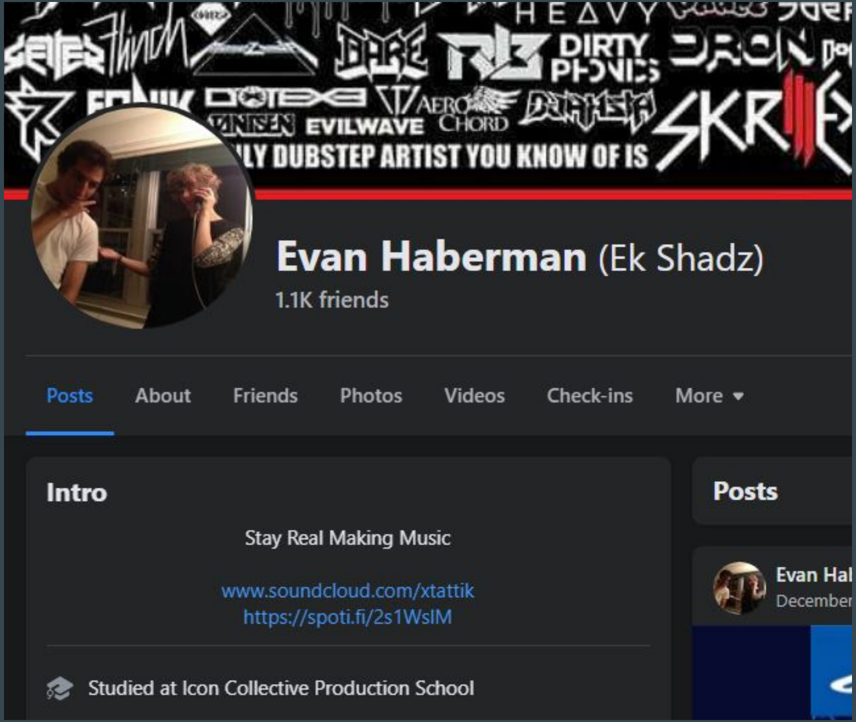


@xtattik

xtattik

@xtattik

xtattik



Evan Haberman (Ek Shadz)

1.1K friends

Intro

Stay Real Making Music

www.soundcloud.com/xtattik
https://spoti.fi/2s1WsIM

Studied at Icon Collective Production School

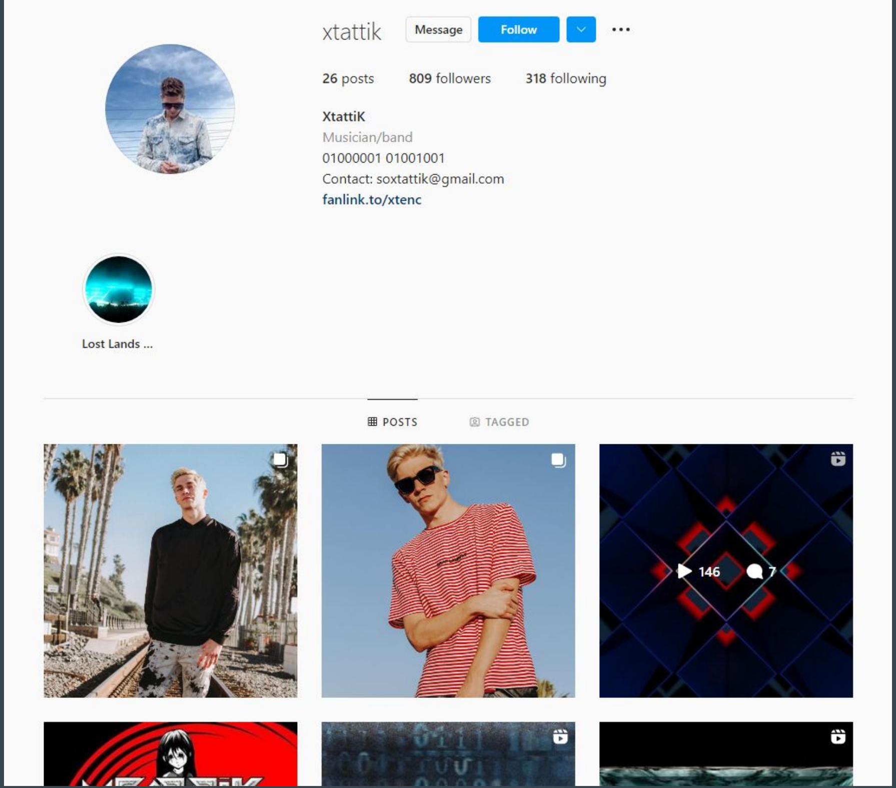
Posts

Evan Hal
December

Recon

Looks like he’s really into music, even making his own!

There are a few posts about Lost Lands...



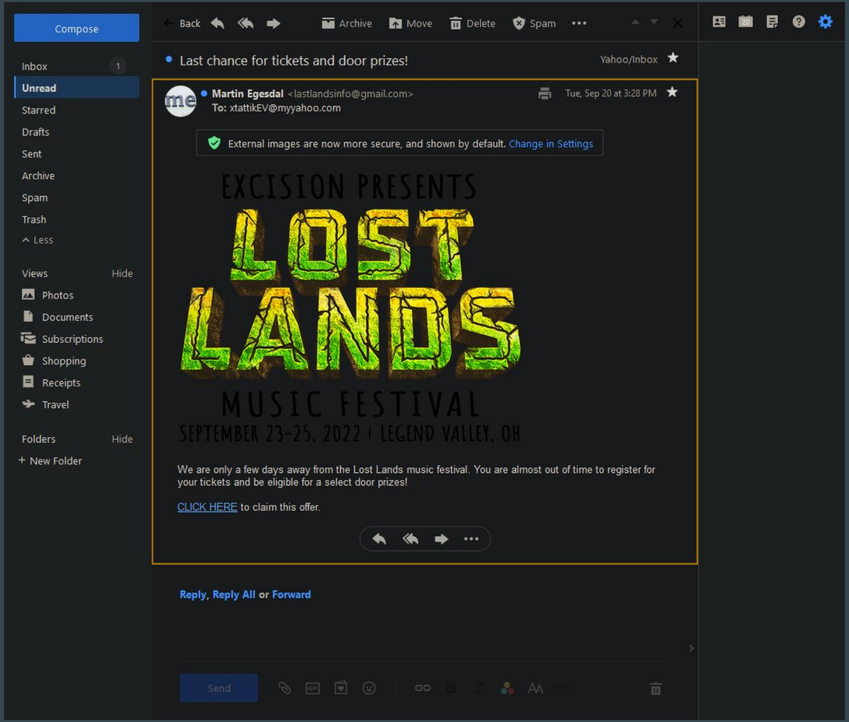
xtattik

26 posts 809 followers 318 following

XtattiK
Musician/band
01000001 01001001
Contact: soxtattik@gmail.com
fanlink.to/xtenc

The Bait

- The attacking email is sent! Now to see if they take the bait.
- This included an image to make the email and offer seem legitimate, as well as a hyperlink to the spoofed website.
- When the target clicks the banner on the spoofed website, it downloads malware that will encrypt their machine.



Last chance for tickets and door prizes!

Martin Egesdal <lastlandsinfo@gmail.com>
To: xtattikEV@myyahoo.com
Tue, Sep 20 at 3:28 PM

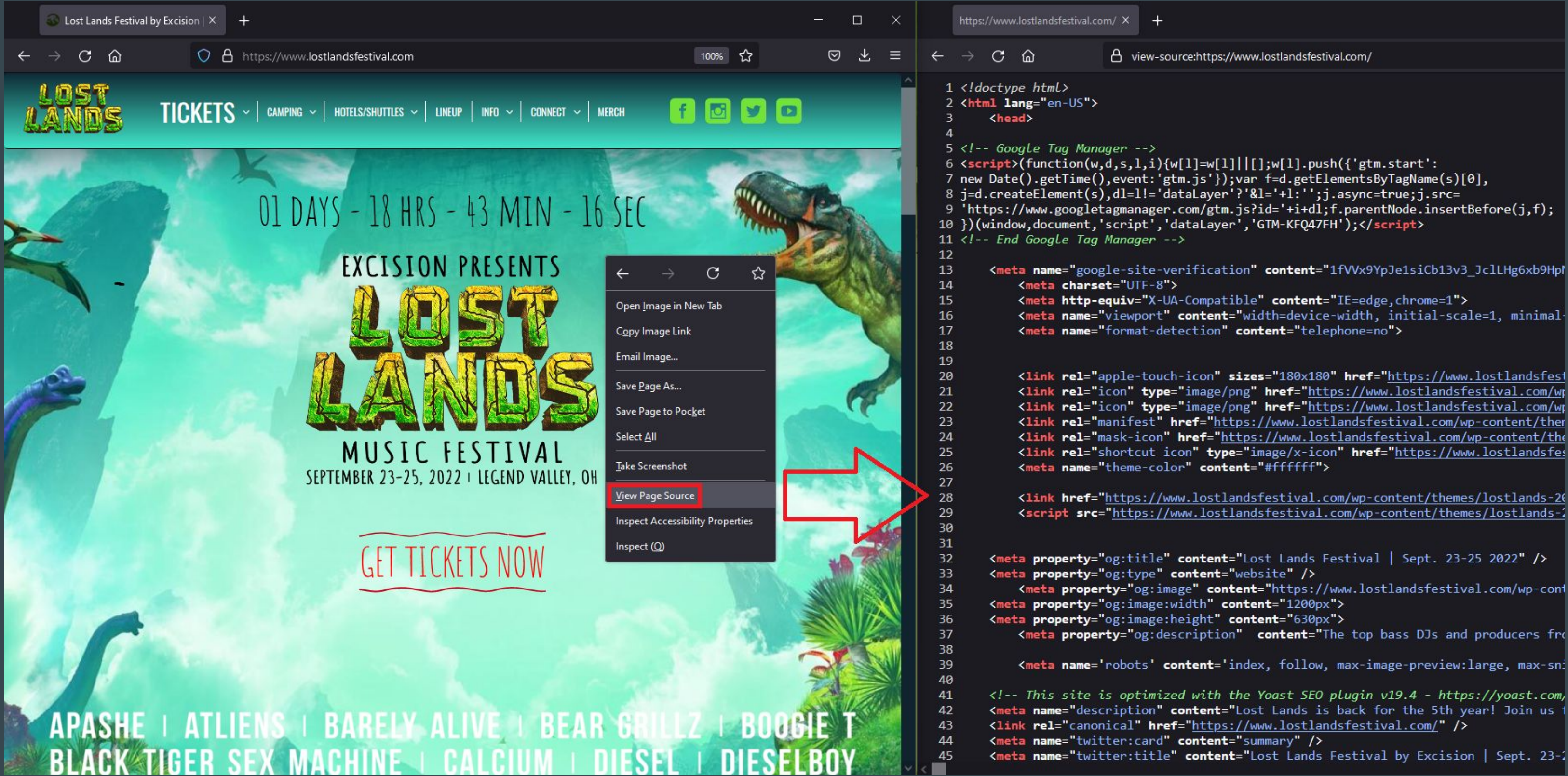
External images are now more secure, and shown by default. Change in Settings

We are only a few days away from the Lost Lands music festival. You are almost out of time to register for your tickets and be eligible for a select door prizes!

CLICK HERE to claim this offer.

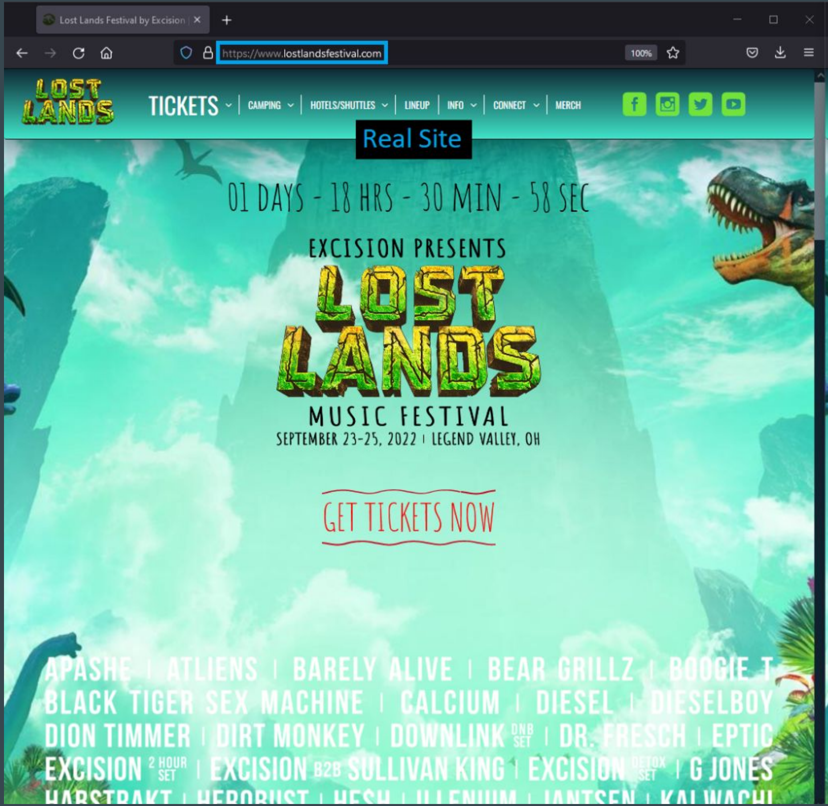
Reply, Reply All or Forward

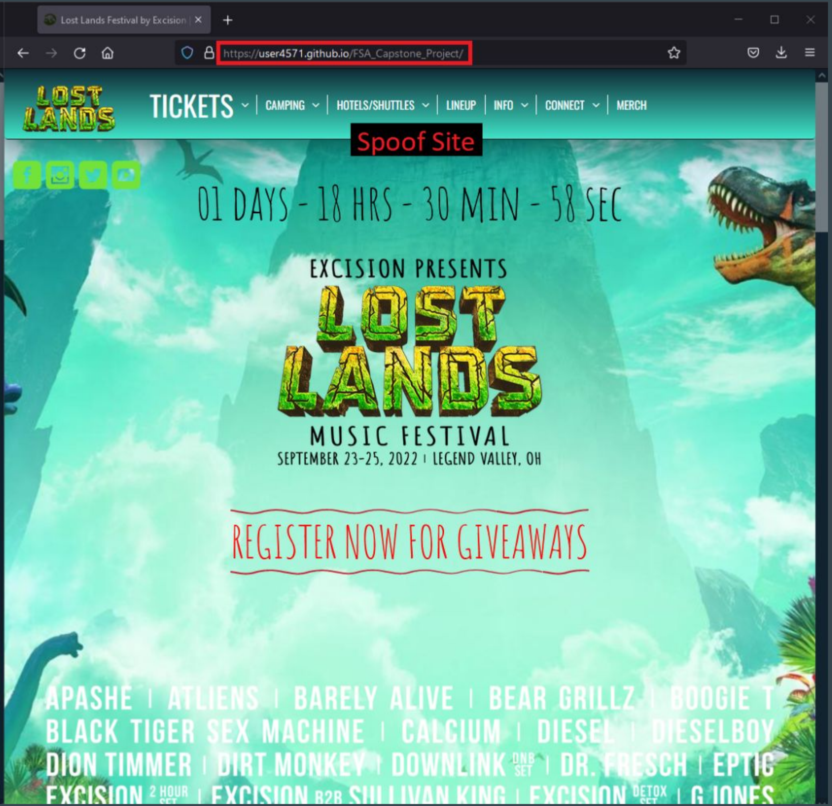
The Switch


Lost Lands Festival by Excision
https://www.lostlandsfestival.com
100%
LOST LANDS
TICKETS
CAMPING
HOTELS/SHUTTLES
LINEUP
INFO
CONNECT
MERCH
01 DAYS - 18 HRS - 43 MIN - 16 SEC
EXCISION PRESENTS
LOST LANDS
MUSIC FESTIVAL
SEPTEMBER 23-25, 2022 | LEGEND VALLEY, OH
GET TICKETS NOW
APASHE | ATLIENS | BARELY ALIVE | BEAR GRILLZ | BOOGIE T
BLACK TIGER SEX MACHINE | CALCIUM | DIESEL | DIESELBOY
Open Image in New Tab
Copy Image Link
Email Image...
Save Page As...
Save Page to Pocket
Select All
Take Screenshot
View Page Source
Inspect Accessibility Properties
Inspect (Q)
https://www.lostlandsfestival.com/
view-source:https://www.lostlandsfestival.com/

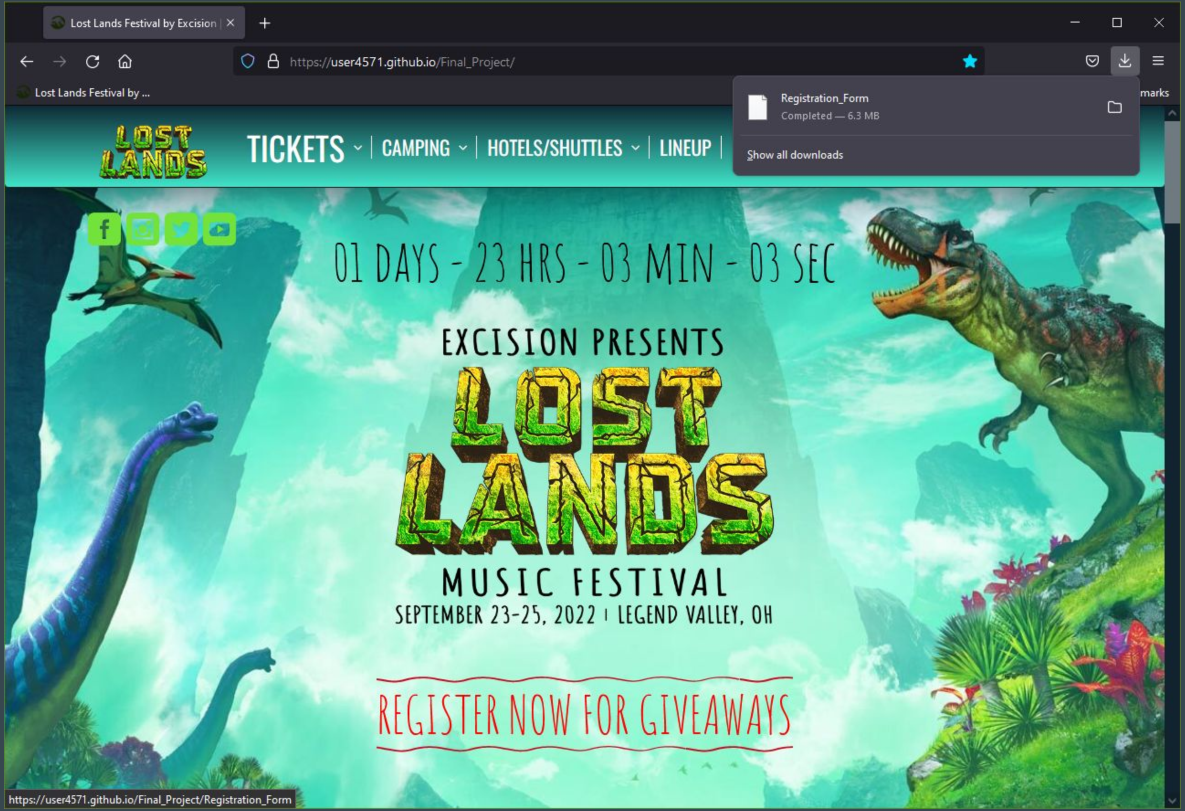
```
<!doctype html>
<html lang="en-US">
    <head>

<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-KFQ47FH');</script>
<!-- End Google Tag Manager -->

    <meta name="google-site-verification" content="1fVVx9YpJe1siCb13v3_JclLHg6xb9Hp
        <meta charset="UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
        <meta name="viewport" content="width=device-width, initial-scale=1, minimal
        <meta name="format-detection" content="telephone=no">


        <link rel="apple-touch-icon" sizes="180x180" href="https://www.lostlandsfest
        <link rel="icon" type="image/png" href="https://www.lostlandsfestival.com/wp
        <link rel="icon" type="image/png" href="https://www.lostlandsfestival.com/wp
        <link rel="manifest" href="https://www.lostlandsfestival.com/wp-content/ther
        <link rel="mask-icon" href="https://www.lostlandsfestival.com/wp-content/the
        <link rel="shortcut icon" type="image/x-icon" href="https://www.lostlandsfes
        <meta name="theme-color" content="#ffffff">

        <link href="https://www.lostlandsfestival.com/wp-content/themes/lostlands-20
        <script src="https://www.lostlandsfestival.com/wp-content/themes/lostlands-2


    <meta property="og:title" content="Lost Lands Festival | Sept. 23-25 2022" />
    <meta property="og:type" content="website" />
        <meta property="og:image" content="https://www.lostlandsfestival.com/wp-cont
    <meta property="og:image:width" content="1200px">
    <meta property="og:image:height" content="630px">
        <meta property="og:description"  content="The top bass DJs and producers fr

        <meta name='robots' content='index, follow, max-image-preview:large, max-sn

    <!-- This site is optimized with the Yoast SEO plugin v19.4 - https://yoast.com
    <meta name="description" content="Lost Lands is back for the 5th year! Join us
    <link rel="canonical" href="https://www.lostlandsfestival.com/" />
    <meta name="twitter:card" content="summary" />
    <meta name="twitter:title" content="Lost Lands Festival by Excision | Sept. 23-
```

The Switch


Lost Lands Festival by Excision
https://www.lostlandsfestival.com
100%
LOST LANDS
TICKETS
CAMPING
HOTELS/SHUTTLES
LINEUP
INFO
CONNECT
MERCH
Real Site
01 DAYS - 18 HRS - 30 MIN - 58 SEC
EXCISION PRESENTS
LOST LANDS
MUSIC FESTIVAL
SEPTEMBER 23-25, 2022 | LEGEND VALLEY, OH
GET TICKETS NOW
APASHE | ATLIENS | BARELY ALIVE | BEAR GRILLZ | BOOGIE T
BLACK TIGER SEX MACHINE | CALCIUM | DIESEL | DIESELBOY
DION TIMMER | DIRT MONKEY | DOWNLINK DNB SET | DR. FRESCH | EPTIC
EXCISION 2 HOUR SET | EXCISION B2B SULLIVAN KING | EXCISION DETOX SET | G JONES


Lost Lands Festival by Excision
https://user4571.github.io/FSA_Capstone_Project/
LOST LANDS
TICKETS
CAMPING
HOTELS/SHUTTLES
LINEUP
INFO
CONNECT
MERCH
Spoof Site
01 DAYS - 18 HRS - 30 MIN - 58 SEC
EXCISION PRESENTS
LOST LANDS
MUSIC FESTIVAL
SEPTEMBER 23-25, 2022 | LEGEND VALLEY, OH
REGISTER NOW FOR GIVEAWAYS
APASHE | ATLIENS | BARELY ALIVE | BEAR GRILLZ | BOOGIE T
BLACK TIGER SEX MACHINE | CALCIUM | DIESEL | DIESELBOY
DION TIMMER | DIRT MONKEY | DOWNLINK DNB SET | DR. FRESCH | EPTIC

The Switch



Lost Lands Festival by Excision |
https://user4571.github.io/Final_Project/
Lost Lands Festival by ...
Registration_Form
Completed — 6.3 MB
Show all downloads
marks
LOST LANDS
TICKETS
CAMPING
HOTELS/SHUTTLES
LINEUP
01 DAYS - 23 HRS - 03 MIN - 03 SEC
EXCISION PRESENTS
LOST LANDS
MUSIC FESTIVAL
SEPTEMBER 23-25, 2022 | LEGEND VALLEY, OH
REGISTER NOW FOR GIVEAWAYS
https://user4571.github.io/Final_Project/Registration_Form

Prevention

- Multi-factor Authorization
- Email Security Software
- Security Awareness Training

Thank You for Watching!

/tristankhim

/talenflippo

/george-a-kell

/olearyrb

/rodney-ramirez

Special thank you to Evan!