We Specialize in One Thing:
*Cybersecurity. Period.*

# Social Engineering

## A Proactive Security

**PRESENTED BY:**
**Stephanie Carruthers**
**Social Engineering Lead**

**MindPoint Group, LLC**
1330 Braddock Place, Suite 600, Alexandria VA 22314
(o) 703.636.2033 | (f) 866.761.7457 | **www.mindpointgroup.com**

## Part II - Open-Source Intelligence

## CONTENTS

## OPEN-SOURCE INTELLIGENCE

> *“Most scams work because victims are successfully convinced the scam is real. Thus, victims give criminals their information more often than it is maliciously stolen. A scammer’s main goal is to convince you to hand over your information voluntarily, as opposed to using forceful intimidation or threats.*
>
> *While hostility is one social engineering methodology, expert scammers know they will be most successful if they gain your trust.* ***Identity thieves do their homework on your interests, business relationships, demographics, behaviors and other personal details before targeting you in a scam to align with these elements****.* ***The research and strategy that goes into planning a scam attack is what social engineering is all about.****”* (Fighting Identity Crimes, 2017)

Have you ever wondered where cybercriminals get their information? What is their starting point? Open-Source Intelligence (OSINT) is an increasingly popular tactic that hackers are using to target organizations and their employees. OSINT is the act of scraping data from publicly available sources. Attackers use the data obtained from OSINT gathering to craft realistic social engineering campaigns.

Some examples of open-source channels used are:

- Internet (search engines)
- Social Media
- Blog Posts
- Online Forums
- Video Sharing Sites (YouTube, etc.)
- Magazines
- Newspapers
- Radio
- TV
- Maps

> ***“While there was no hack involved, the Cambridge Analytica debacle is a form of social engineering – a method information operation used to trick human beings into giving away sensitive information, without exploiting the computer system or network in question.” (Fighting Identity Crimes, 2017)***

Attackers use several tools and websites to conduct OSINT gathering, including Google Dorking, namechk.com and Glassdoor, which will be further explained in the sections below. Once the information is discovered, attackers craft custom attack vectors against organizations or employees. In this whitepaper, we’ll further expand on how attackers conduct OSINT and what they can do with the information obtained and review the necessary measures you should be taking to prevent the attacks.

## ORGANIZATION-FOCUSED ATTACKS

Attackers utilize several attack vectors to take advantage of an organization, including large-scale phishing campaigns, network hacking, application hacking, or even a physical intrusion. Attackers typically look for this type of information:

- email addresses
- phone numbers
- vendors
- internal documents

- physical security information
- intellectual property
- organizational sensitive information

## EMPLOYEE-FOCUSED ATTACKS

Another method attackers use is targeting an individual employee through spear phishing, vishing, or in person. Using this approach, attackers typically mine for contact information such as:

- phone numbers
- email addresses
- home addresses
- work addresses
- other information (interests, relationships, job functions)

In other cases, OSINT can be used to gain answers to security questions or hints for password cracking.

Want to see how OSINT gathering can be found easily for yourself? Look at one of your friend's social media profiles. Is their account public, exposing its content to everyone? Do they have any of the following information on their profile: children's names, pet names, birthday, anniversary, place of birth, hobbies, relatives, favorite sport teams, phone numbers, or even an address? This data is the type of information that can be easily found via OSINT gathering and used in targeted attacks.

## HOW DO ATTACKERS DO IT?

For attackers to have successful social engineering campaigns, utilizing OSINT gathering is a must. Information discovered while OSINT gathering can make or break a campaign.

OSINT data may be gathered manually by using a search engine or reviewing a company's website. While manual methods often provide the best information, automated tools such as theHarvester provide an automated avenue for data gathering. Regardless of the method used, the gathered data should be reviewed to identify if any sensitive information was obtained.

Below are some of the OSINT data gathering methods used by attackers.

## TOOLS AND WEBSITES USED FOR OSINT

Surprisingly, there are numerous free or inexpensive online tools that make it easy to access sensitive information about an individual. Websites such as Pipl.com or Namechk.com make money by selling personal information to strangers on the internet. Hackers may use one or all of the tools listed below to obtain your personal information and those of your employees, too.

Social media sites are breeding grounds for sensitive information. Many attackers simply log in and do a quick search to find a user's public profile, which is already pre-populated with all the information they need. Below are different tools, websites and social media platforms used for OSINT.

| Some OSINT Tools | |
|---|---|
| FOCA | Maltego |
| Google Dorking | Shodan |
| Recon-ng | theHarvester |
| Urlcrazy | SpiderFoot |

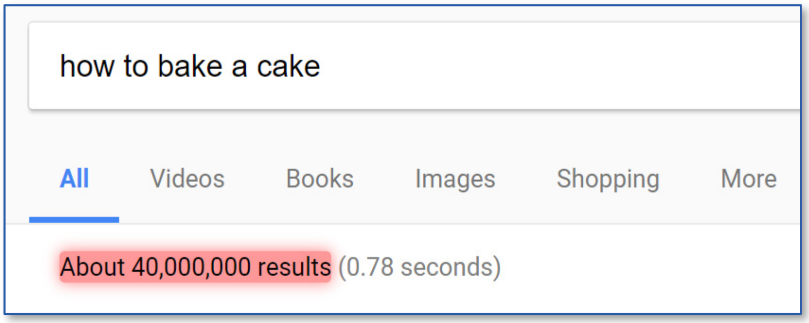
| Useful OSINT Websites | |
|---|---|
| pipl.com | spokeo.com |
| namechk.com | tineye.com |
| archive.org/web | inteltechniques.com |
| email-format.com | osintframework.com |
| haveibeenpwned.com | google.com/maps |
| familytreenow.com | research.com |

| Social Media | |
|---|---|
| LinkedIn | Facebook |
| Twitter | Instagram |
| Pinterest | Myspace |
| Google Plus | Flickr |
| Meetup | Glassdoor |

## GOOGLE DORKING

Google Dorking, also called a Google Hack, is an advanced search query that assists in finding information that a normal search would not. Google Dorking can be utilized to identify sensitive documents or information.

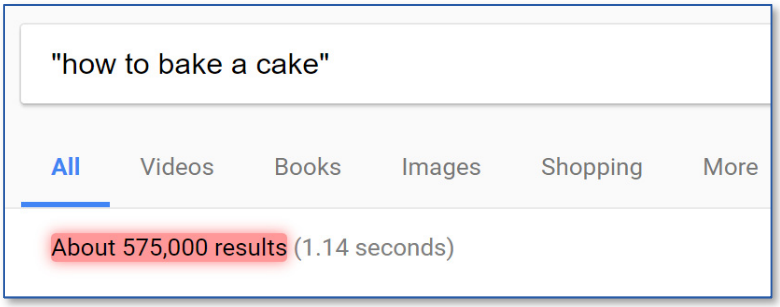
A regular search returns many results based on different combinations of the words in your query. For example, a search for "how to bake a cake" returns about 40 million results:



how to bake a cake

About 40,000,000 results (0.78 seconds)

However, if we put the search term in quotes, Google will search for the EXACT phrase, narrowing down our search results to a more manageable 575 thousand. These quotes are called a search operator (a special symbol or keyword that makes the search more specific).


"how to bake a cake"

About 575,000 results (1.14 seconds)

Some other common Google Dorking search operators are listed below:

| Operator | Function |
|---|---|
| site | Search specific site |
| filetype | specific files |
| intext | Search text of page only |
| inurl | Search URL |
| * | Wild card for a single word |
| “ “ | Searches for exact phrase |
| + | Returns common words that might ordinarily be discarded |
| - | Removes pages that mention a given term |

When using operators, make sure to remove any spaces between the operator and query.

*Example of trying to find content that is only on amazon.com using the site operator:*

- site:amazon.com

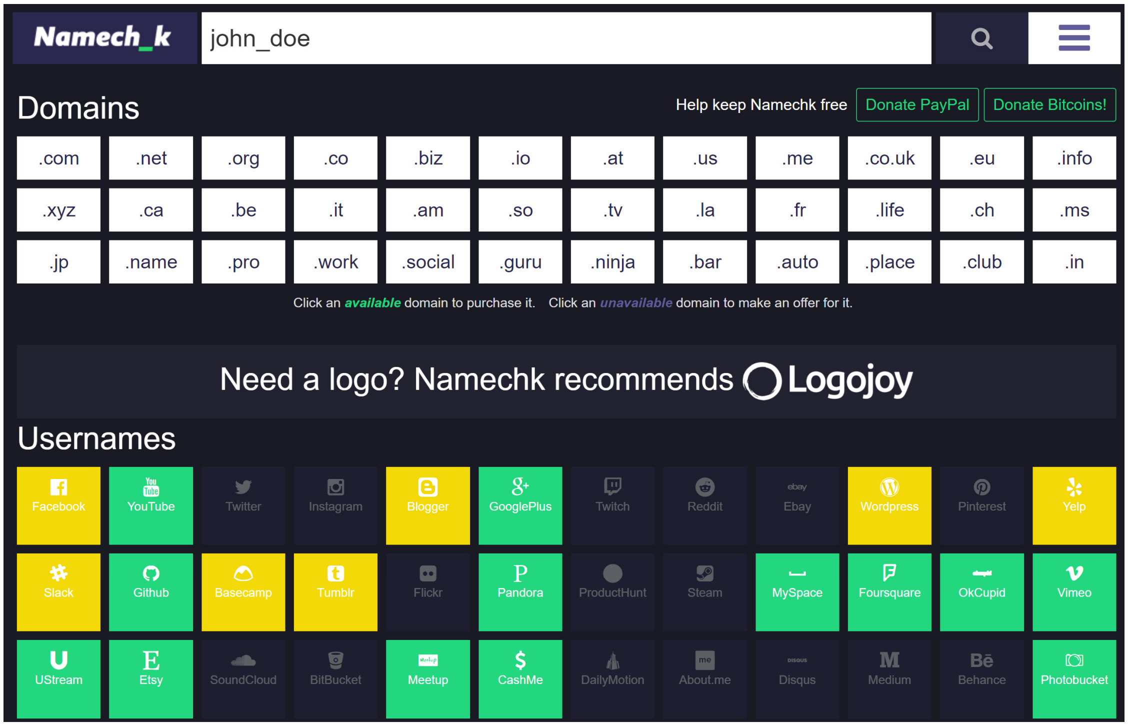
You can also combine operators together for more control over your search. The following are examples of Google Dorking operators often used in OSINT. Find more examples here.

- website:targetcompanywebsite.com “employee login”
  *These commands search for the exact words “employee login” on targetwebsite.com*
- website:targetcompanywebsite.com  filetype:PDF “employee handbook” +security
  *These commands search for PDF files on the website targetwebsite.com with the exact words “employee handbook” which also has to include the word security*

## NAMECHK.COM

Typically, when someone chooses a username for a social media website, they are more likely to keep that same username across multiple platforms. When performing OSINT gathering against an individual, if a username is discovered, the website namechk.com can come in handy. When provided with a specific username, namechk.com runs the username through many websites and domains to see if that username is already being used elsewhere. This service helps identify multiple accounts used by the target, which may net the attacker new pieces of intelligence to analyze, such as additional social media accounts, video sharing sites, blog posts, etc.

The image below displays the search for the username "john_doe". The greyed-out icons indicate that the username is already in use on that website. Additionally, if you click on the greyed-out icon, it directly takes you to the website for that username.



Namech_k john_doe

Domains

Help keep Namechk free Donate PayPal Donate Bitcoins!

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| .com | .net | .org | .co | .biz | .io | .at | .us | .me | .co.uk | .eu | .info |
| .xyz | .ca | .be | .it | .am | .so | .tv | .la | .fr | .life | .ch | .ms |
| .jp | .name | .pro | .work | .social | .guru | .ninja | .bar | .auto | .place | .club | .in |

Click an *available* domain to purchase it. Click an *unavailable* domain to make an offer for it.

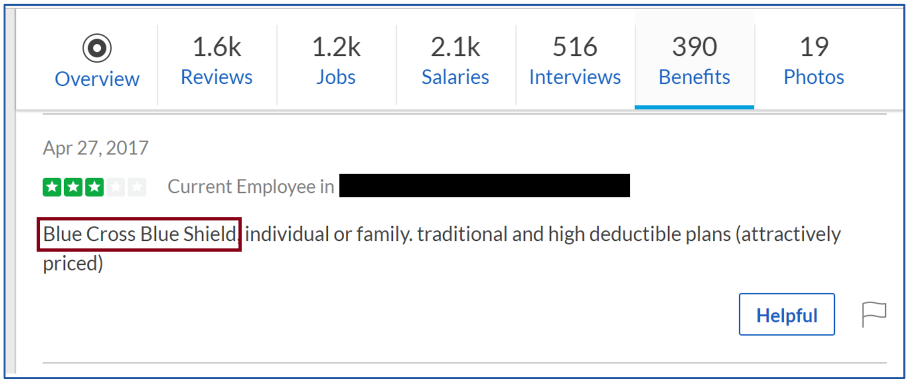
Need a logo? Namechk recommends Logojoy

Usernames

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Facebook | YouTube | Twitter | Instagram | Blogger | GooglePlus | Twitch | Reddit | Ebay | Wordpress | Pinterest | Yelp |
| Slack | Github | Basecamp | Tumblr | Flickr | Pandora | ProductHunt | Steam | MySpace | Foursquare | OkCupid | Vimeo |
| UStream | Etsy | SoundCloud | BitBucket | Meetup | CashMe | DailyMotion | About.me | Disqus | Medium | Behance | Photobucket |

## GLASSDOOR

When performing OSINT against an organization, Glassdoor provides internal organizational information such as: medical benefit providers, company pictures, job titles, pay information, and more. With the knowledge of medical benefit providers, the attacker can craft a phishing campaign to individuals, claiming to be from the medical benefit company.



Apr 27, 2017

★★★☆☆ Current Employee in [redacted]

Blue Cross Blue Shield individual or family. traditional and high deductible plans (attractively priced)

## WHAT CAN ATTACKERS DO WITH THIS INFORMATION?

OSINT gives attackers the information they need to launch a campaign on your organization and employees. These attacks can range from social engineering vectors (spear phishing emails, vishing calls, physical security) to network or application attacks.

To provide you with an idea of the damage OSINT can cause, below are scenarios where attackers will utilize OSINT information obtained to give you an idea of the damage OSINT can cause.

## DEVELOP A PHISHING CAMPAIGN

### ATTACKER'S GOAL

The goal of the attacker is to gain as many employee email addresses as possible, which allow the attacker to conduct a phishing campaign. The end goal of the phishing campaign is harvesting employee credentials, eliciting sensitive information, or having employees download a malicious attachment.

### METHOD

There are multiple steps an attacker can take to gather as many email addresses as possible and develop pretext information.

1. The attacker searches for email addresses using TheHarvester against their targeted organizations domain name.
2. The attacker can additionally identify the email address format using john_doe@<company name>.com. Next, the attacker can scrape employee names from social media websites and combine them with the email format to make a list of employee email addresses.
3. With a list of target email addresses ready, the attacker will plan their pretext. In order to determine who they want to impersonate, the attacker may search for third-party associates of the organization by investigating the organization's website, reading through Glassdoor, or possibly utilizing google dorks.
4. Finally, with a pretext selected, the attacker will pick which type of attack they will utilize. For example, if the attacker decided to impersonate a third-party association, like a medical benefits company, the phishing email can direct targets to a malicious website stating they need to review and approve their most recent claim.

## STEAL AN EXECUTIVE EMPLOYEE'S LAPTOP

### ATTACKER'S GOAL

The attacker's goal is to gain access to an executive employee's laptop.

### METHOD

The attacker starts by finding the employee's social media accounts. Investigations of these accounts may expose the employee's work hours and the time they have their lunch break by looking at the timestamps on their posted pictures.

A sophisticated attacker doesn't stop at the employee. They will also gain intelligence on the physical security of the building. For example, once the attacker finds the company's YouTube account, they may be able to find videos of the building's security, employee badges, dress code, and other sensitive information.

Finally, the attacker searches social media accounts to try to find an image of a company badge. One employee may absentmindedly upload a photo of their badge at work, which the attacker uses to make a replica. When the targeted employee takes their lunch break, the attacker uses the fake employee badge to gain access to the appropriate floor and the target laptop.

Alternatively, if the employees typical work hours or lunch breaks cannot be identified, the attacker can still create a replicate employee badge, but show up later in the work day, and wait for employees to leave the building.

## HOW CAN I PREVENT AN ATTACK?

The first step to preventing an attack is arming yourself with knowledge. By reading this paper, you have already gained a good understanding of OSINT, what kind of information is most vulnerable, and how hackers use OSINT to attack your organization and employees.

Now that you know why OSINT is dangerous, you need to prevent it. The best course of action is to conduct OSINT assessments against your own organization. These assessments allow you to identify your vulnerabilities and remediate or mitigate them before they are exposed to the wrong eyes.

However, you should not rely solely on your self-observation. It is important to bring in an outside specialist at least once a year to perform assessments of your company's security. An outside specialist can bring fresh eyes to your company and find vulnerabilities that you may be overlooking. Your own assessments may make you immune to internal issues or company politics that could be compromising your security measures.

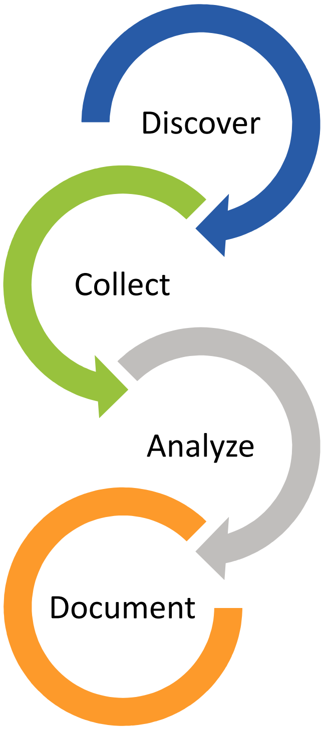
Finally, be smart when online and encourage your employees to do the same. Keep your exposure to an absolute minimum by keeping social media profiles private, refraining from publicly discussing your company or its sensitive information online, and removing details from LinkedIn accounts.

If you think your information is already safe from the public eye, run a quick search of your name or email on the websites identified on page 3. You may be surprised at what you find.

The key takeaway is that the internet is a big place, and information travels fast. Do not underestimate the data-mining skills of determined and sophisticated attackers. Start taking steps today to protect yourself, your organization, and employees.

## MINDPOINT GROUP'S OSINT METHODOLOGY

MindPoint Group (MPG) utilizes a four-point methodology when performing OSINT assessments. MPG often discovers information that our clients do not realize is available to the public, leaving our clients with a prioritized list of findings to remediate before an attacker can the vulnerabilities use to their advantage.



- **Discover:** First, MPG **discovers** data that could be exploited by attackers. This is typically sensitive or important information for your organization's operations such as internal IT structure or even physical security in place.
- **Collect:** Next, MPG **collects** volumes of data identified during the **discover** phase by utilizing free, open-source channels. MPG will mine data both manually and with the help of automated processes to cover all possible avenues a true attacker would utilize.
- **Analyze**: MPG will **analyze** all of the collected data to uncover any sensitive information that may have been revealed.
- **Document**: All potentially harmful information will be documented according to the level of risk.

## NOW WHAT?

So far in our series, we have discussed the history of social engineering in Part One: A Dirty Old Trick as well as the importance of OSINT and the threat it poses to organizations and individuals alike in this whitepaper. However, that is not the end of the security story. Future whitepapers in this social engineering series will cover multiple social engineering vehicles (phishing, vishing, and physical security) as well as how you can mitigate risk to your company from these attacks. The upcoming parts of the series will include the following topics:

- Part Three: Phishing
- Part Four: Vishing
- Part Five: Physical Security
- Part Six: How to Lower Your Risks to Social Engineering Attack

## ABOUT MINDPOINT GROUP

MindPoint Group is a cybersecurity consulting firm providing innovative solutions including:

- Cloud Security
- FedRAMP 3PAO Services
- Proactive Security
- Security Architecture & Engineering
- Security Operations
- Governance, Risk & Compliance
- Managed Security Services

MindPoint Group's Proactive Security Services offers social engineering solutions led by Subject Matter Experts. Our methodology is focused on providing customizable White Box (Insider Threat Simulation) and Black Box (Adversarial Simulation) assessments to meet the unique requirements of our clients. Our Social Engineering assessment and audit services range from Open-Source Intelligence, Phishing, Vishing, Physical Security Assessment, and Physical Security Audit.

## ABOUT THE AUTHOR

Stephanie Carruthers is a Social Engineer Team Lead at MindPoint Group. After winning a black badge at DEF CON 22 for the Social Engineering Capture The Flag (SECTF), Stephanie Carruthers pursued her career as a full time Social Engineer. Stephanie focuses on services such as Open-Source Intelligence (OSINT) gathering, Phishing, Vishing, and Physical security assessments. Stephanie also was on the winning team for SAINTCON'S Vault Physical Security challenge, which won the team a black badge. Over the last five years Stephanie has presented and taught trainings at multiple security conferences including BSidesSLC, CircleCityCon, SAINTCON, ISACA (Salt Lake City), Hackfest Canada, and NolaCon. Stephanie has performed a variety of Social Engineering assessments for clients ranging from start-ups, Fortune 100 companies, to government agencies. Stephanie is on the DEF CON CFP review board as a specialist for Social Engineering submissions.

## LEARN MORE

For additional information about our cybersecurity services, please visit our website and social media:

- mindpointgroup.com
- LinkedIn
- Twitter
- GitHub
- Glassdoor
- Facebook

To learn more about MindPoint Group's Social Engineering services, please email Stephanie and the Proactive Security team at: pss@mindpointgroup.com