

Assignment 1: Go Phish

Megan Kaczanowski, Ravi Kohli, Suraj Khadka, Bryan Kim

Objective & Value: Conduct Email Spear Phishing Campaign

- Team 19's campaign was a **spear phishing campaign** targeted at PUBP6725 Teaching Assistant Michael Brown (mbrown337@gatech.edu). Given that we're attempting to target a specific individual, a spear phishing (highly custom, targeted campaign) is our best option.
- Our objective was to deliver an email with an attachment (in a real-world scenario, the bad actor would have delivered malware to the user's device, though as this is an educational campaign, we opted to simulate this impact).
 - As a malicious actor, we would have leveraged spyware with a keylogger to steal the user's credentials to sensitive sites like their bank account, other financial accounts (particularly cryptocurrency wallets), and primary email address.

Desired Data, Damage & Markets

In a real-world scenario, a bad actor would have delivered malware to the user's device, though as this is an educational campaign, we opted to simulate this impact. Ideally, the malware we delivered would have been spyware, with a keylogger to steal sensitive login information (like bank account credentials).

There are two routes we could pursue here - either leveraging stolen credentials ourselves, or selling the credentials to a third party.

- Pursuing exploitation of stolen data/credentials
 - Depending on what we were able to capture, we can pursue additional attack techniques. With email credentials, we would want to immediately try resetting our target's passwords for other accounts, sending spear phishing emails to the target's family and friends (in order to expand the scope of our influence and gather additional credentials), and trying to login to the target's financial accounts (such as cryptocurrency wallets and bank accounts and making transfers of these accounts to accounts we control). This is particularly effective for cryptocurrency accounts as they don't require the same amount of oversight as traditional financial instruments and don't have the same fraud controls from a central authority.
- Selling the credentials
 - There are a number of dark web marketplaces where you can sell user data, though this list often changes as marketplaces are shut down by law enforcement agencies (such as the Silk Road, ToRReZ, UniCC, Hydra Market, etc.). We could choose to sell the exploited credentials on one of these sites (Genesis Market, 2Easy, OMG!OMG!, etc), though typically that would be more effective for a large dump of credentials, not for a specific spear phishing attack. Given that credentials sell for hundreds to thousands of dollars, it isn't an effective business model to spend a lot of time spear phishing a specific target and just selling the credentials (this option would make more sense with mass campaigns), so a malicious actor is more likely to pursue the first option).

Campaign Purpose & Intended Outcome

Purpose:

Our campaign aims to specifically target Michael Brown, based on information we've gathered about him (a likely recipient of VA benefits), with the intention of getting him to open an attachment with malware and download it to his device. The malware would be spyware which could be leveraged to steal the target's credentials to sensitive sites.

Outcome:

This stolen information would be leveraged for subsequent attacks (described in the previous slide in more detail), or sold on various dark web marketplaces for immediate benefit.

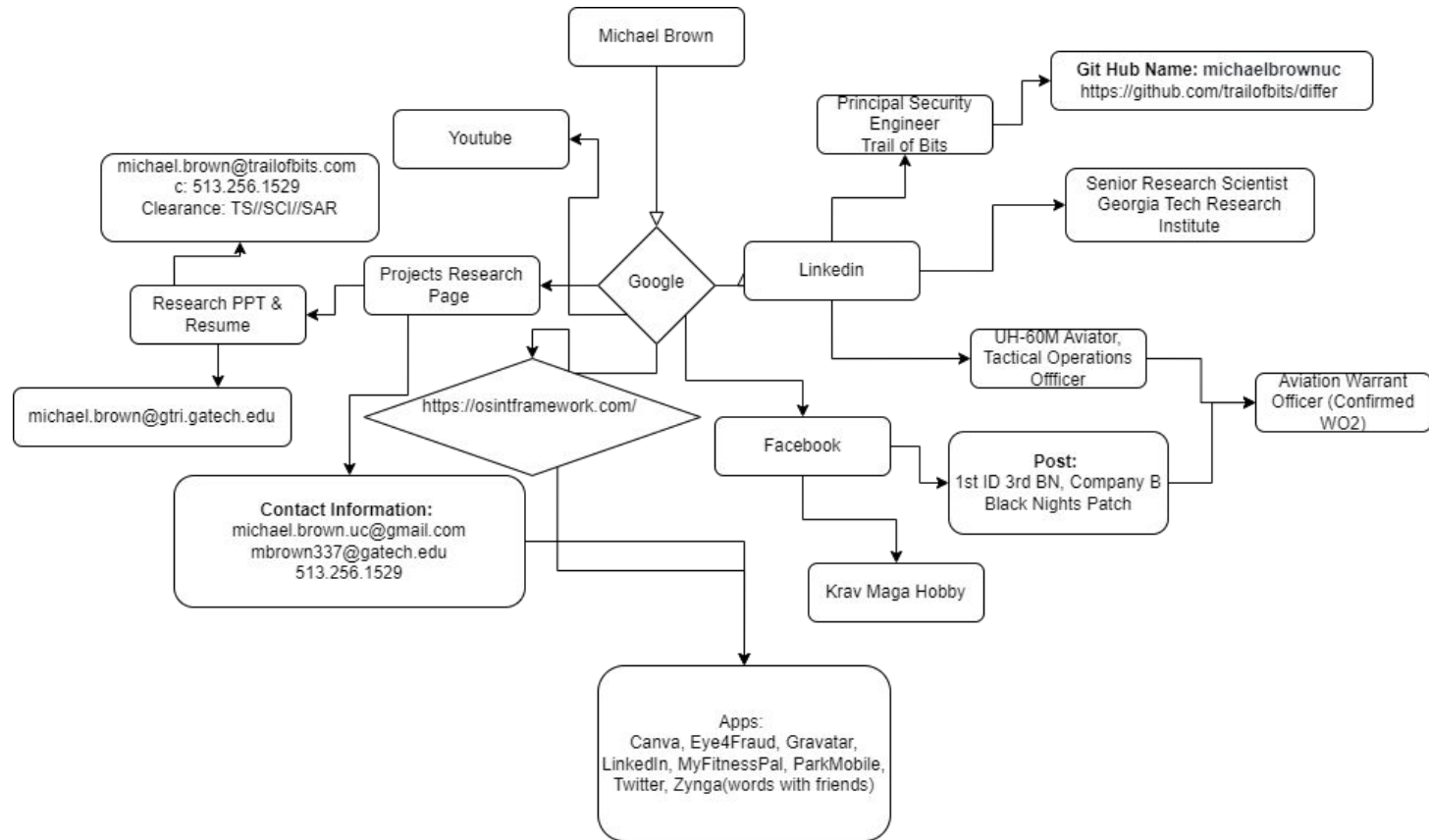
The Target: Michael Brown

Reconnaissance:

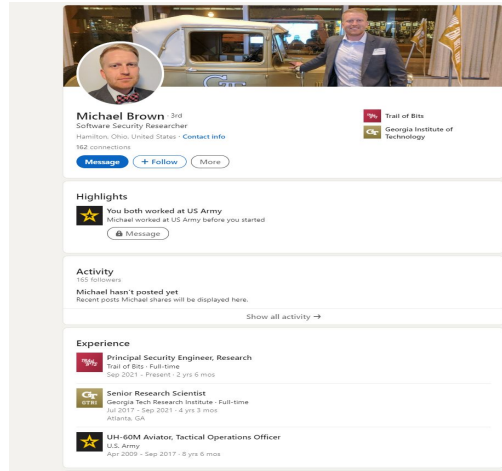
In order to ascertain the best approach to spear phish the target, we performed OSINT (open source intelligence) research, in order to gather the following information:

- Determine the contact information, professional history of the target, personal interests, and history
- Gather information using OSINT sources
 - Google Dorks, Google Reverse Image Searches
 - HaveIBeenPwned
 - Social Media Sites
 - Additional OSINT research, based on the framework outlined in Michael Bazzell's book (Hiding from the Internet)
- Draw conclusions based on data gathered in order to create a phish targeted to Michael Brown.

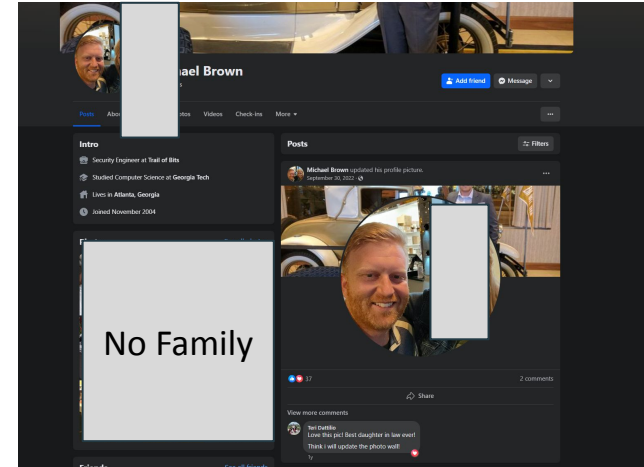
Social Network Map of Michael Brown



Social Media



LinkedIn



Facebook Page



Personal & Research Page

Target Information

From our OSINT we found that our target was on active duty for 8 years in the US army, where he served as a UH-60M Aviator Tactical Operations Officer and Aviation Mission Survivability Officer in the 1st infantry division 3rd BN, Company B, potential rank of CW5 (CW2 in 2013). He has also spoken about his experience several times, including in a feature for [GA tech on 'Life After the Army'](#), and in a panel for [the Atlantic](#), where he was noted as being an army veteran.

Additional Information:

- Currently employed as a Senior Security Engineer, Research Practice for Trail of Bits ([Work Github](#))
- [LinkedIn](#), [Facebook](#), [Personal Website](#)
- Personal Email: michael.brown.uc@gmail.com
- Student Email: mbrown337@gatech.edu, previously michael.brown@gtri.gatech.edu
- Work Email: michael.brown@trailofbits.com | c: 513.256.1529 | Clearance: TS//SCI//SAR
- Personal Phone: 513.256.1529
- Social Apps he uses: Canva, Eye4Fraud, Gravatar, LinkedIn, MyFitnessPal, ParkMobile, Twitter, Zynga(words with friends)
- Hobbies: krav maga

Approach:

Given our target's status as a veteran of the US Army, it is reasonable to assume that they are receiving VA benefits. To exploit this, our spear-phishing email will be crafted to appear as if it originates from the United States Department of Veteran Affairs. This tactic aims to deceive the recipient into believing it's a legitimate inquiry regarding their entitlements and veteran status. By leveraging social engineering techniques, we intend to reduce the target's defenses, enticing them to click on embedded hyperlinks and PDF attachments within the email.

Target Defenses, Vulnerabilities, and Potential Failure Points

Target Defenses: As the target is a Senior Software Security Engineer, he's likely to possess extensive expertise in software security and surpass typical familiarity with email security protocols. In order to combat this, we've leveraged an email which has urgency (this attachment is key to keeping your VA benefits) and familiarity triggers (he's likely emotionally invested in his previous army service, based on how frequently we found that h has been involved with the veteran community in our OSINT research) to hopefully overcome his natural reticence to open unknown attachments.

Target Vulnerabilities: Essentially, in order to overcome our target's defenses, we need to trigger his emotions enough to overcome his natural reticence to click suspicious emails, and we need our email to pass through any spam filters he's leveraging to protect his inbox. In order to do that, we've crafted an email designed to appeal to his emotions about his previous military service (something it seems he cares deeply about based on his social media posts).

Potential Failure Points: Given the target's experience, using an odd sender address, could raise suspicions especially if it differs from his established contacts or corporate norms. Given this, we've leveraged a well-known domain. Finally, the target's cybersecurity experience implies that he might be watchful of dubious attachments, which lowers the possibility of success if the phishing email has any of these components. Given this, we've titled the attachment to seem legitimate, and in line with the tone of the rest of the email.

The Campaign

C2 Node & Backend

- C2 is simulated on a low power ARM platform (Raspberry pi 4B) in order to avoid using a device (like a personal laptop) which is easy to tie back to one of the students

Delivery Platform

- GoPhish platform for launching phishing campaign was used (additional details provided in next slide)
- Utilizing the @fastmail domain to create legitimacy

Payload/Exploit

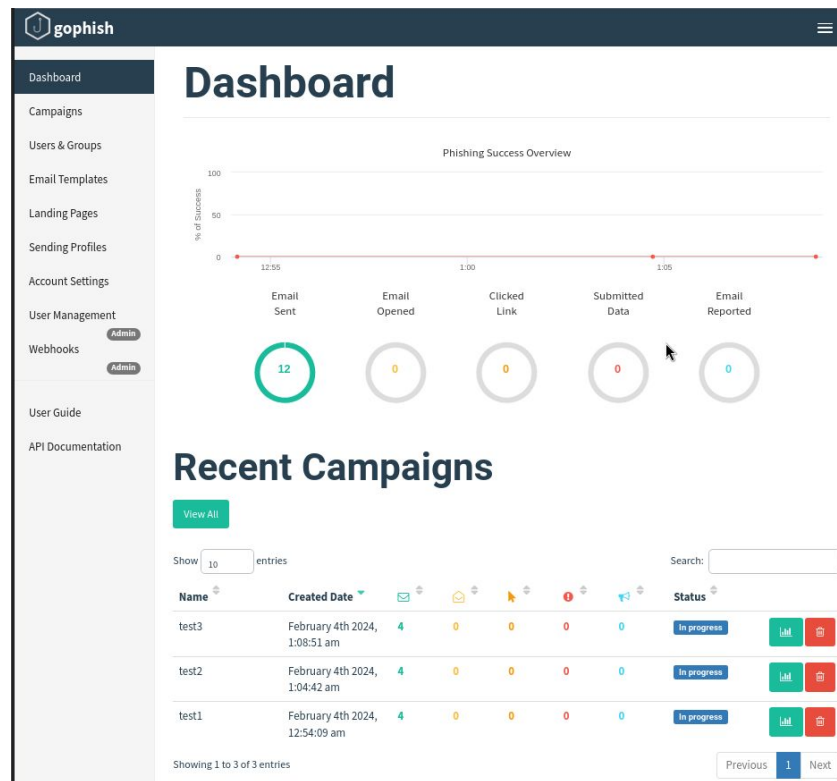
- A PDF infected with Spyware malware is our payload for our phishing email (which we mocked with a fake pdf, but did not leverage real malware given that this is an educational activity)
 - We would have leveraged spyware if we were true malicious actors in order to capture the target's credentials which we could have leveraged for additional gain (details shown in slides above)
- Hypertext link for landing page that is used for fake CAPTCHA/Credentials

Plausible domain

- This phishing campaign is carried out using @fastmail account instead of using fake/specific domain account since fastmail is a trusted domain to most users.

GoPhish 0.10.1 - Tool used for exploit

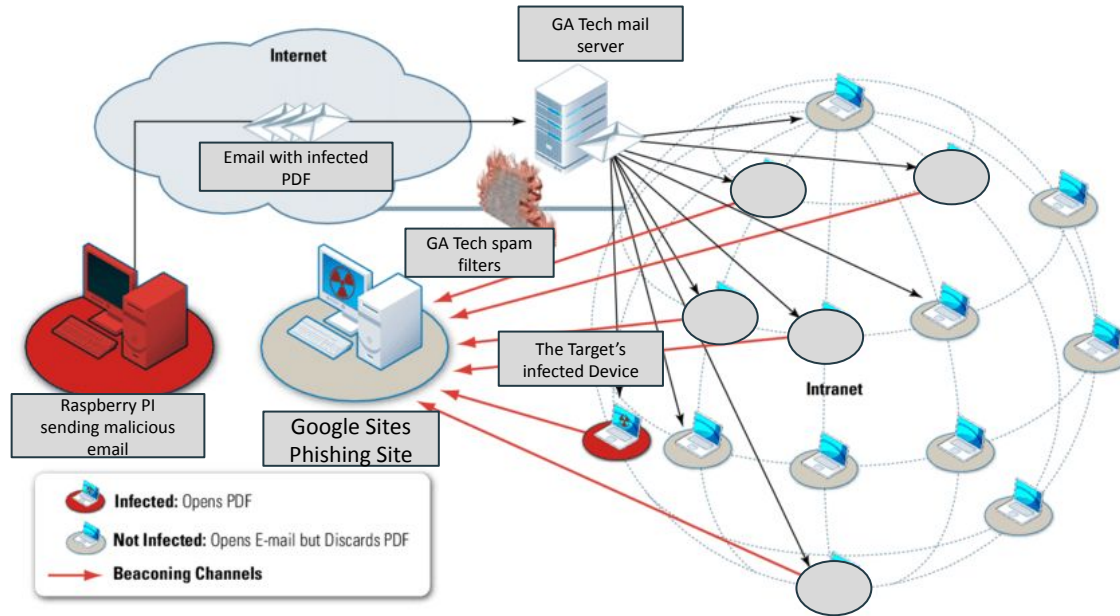
- **Open-source** phishing simulation platform
- Helps organizations test employee susceptibility to phishing attacks
- Creates realistic email campaigns with customizable templates and payloads
- Tracks clicks, opens, and other user interactions to assess awareness levels
- Email campaign creation: Design emails with various templates, sender information, and attachments.
- Landing page customization: Create mock landing pages that mimic real-world phishing targets.
- Reporting and analytics: Track user interactions, identify trends, and measure campaign effectiveness.



C2 Infrastructure:

- Gophish 0.10.1 run on a Raspberry Pi 4B.
- We also tested Kali Linux running native on the Raspberry Pi. Also, we tested in a VM with a prebuilt Kali VM image (Kali Linux 2023.4).
- Additionally, we investigated a scaled campaign. This is a GoPhish feature that provides bulk imports of CSV separated email addresses, which would allow for real world simulation of multiple victim attacks.

Overall Phish Infrastructure



In this case, we're showing the representation of many GA tech users receiving emails from the GA tech mail server, but only a single target (Michael Brown) to whom we're sending a phishing email.

Visual representation of phish infrastructure targeting the TA

Configuration...

The screenshot shows the Gophish web interface. The top navigation bar includes the Gophish logo and a hamburger menu. The left sidebar contains a list of navigation items: Dashboard, Campaigns (selected), Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an Admin button), Webhooks (with an Admin button), User Guide, and API Documentation. The main content area is titled 'Campaigns' and features a '+ New Campaign' button. Below this, there are tabs for 'Active Campaigns' and 'Archived Campaigns'. A search bar and a 'Show 10 entries' dropdown are present. The main table displays a list of campaigns with columns for Name, Created Date, and Status. Each row includes three action icons: a bar chart, a refresh icon, and a trash icon. The table shows three entries, all with a status of 'In progress'. At the bottom, there is a pagination control showing 'Previous', '1', and 'Next'.

Name	Created Date	Status	Actions
test3	February 4th 2024, 1:08:51 am	In progress	
test2	February 4th 2024, 1:04:42 am	In progress	
test1	February 4th 2024, 12:54:09 am	In progress	

- Tested the target's spam filter using multiple phishing campaign exploits
- Gathered campaign failure information
- SMTP configuration

Email Content - Spam Filters and 'Junk' Folder

×

Edit Group

Name:

pubp6725

+ Bulk Import Users

Download CSV Template

First Nc

Last Nc

Email

Position

+ Add

Show

10

entries

Search:

First Name	Last Name	Email	Position
bryan	kim	bkim633@ga...	<div>🗑</div>
megan	kaczanowski	mkaczanows...	<div>🗑</div>
ravi	kohli	rkohli35@ga...	<div>🗑</div>
suraj	khadka	skhadka9@g...	<div>🗑</div>

Showing 1 to 4 of 4 entries

Previous

1

Next

Close

Save changes


✕

Edit Template

Name:

email-pdf

Import Email

Envelope Sender: 


john_doe@cyberresearch.gov










Subject:

Software debloating eval

Text

HTML



B I U       Styles - | Format - |  Source  

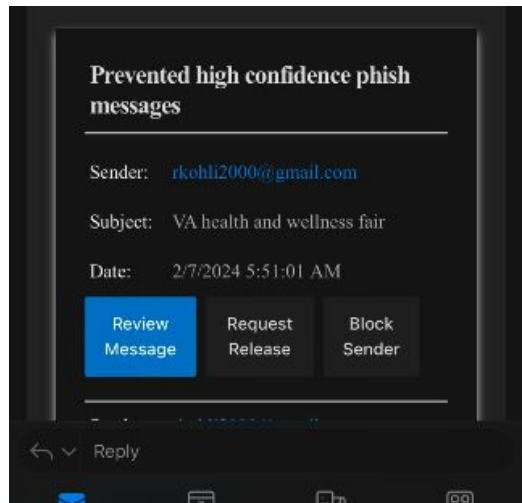
comparative evaluation or software debloating tool; that explores recent breakthroughs in software debloating tools and seeks to improve the program security and performance by removing bloat. I have been working in the area of security and avionics and thought your research on bloat and security improvement lends valuable insights, particularly relating to DAL A level certification of software under DO-178C in aviation. The attached paper highlights this with respect to your research work. It also discusses MC/DC coverage issues and cost analysis. I've attached the PDF for your reference. I'm happy to chat about it further if you're interested and explore potential collaborations or discussions based on these findings as it relates to clear and clearance required work. Best regards, John Doe</p>{{.Tracker}}</body></html>

- Email content tested showed the Outlook365 spam filter more likely to quarantine embedded images or flyers.
- External public email delivered was likely undetected in a 2 stage attack via URL obfuscation.
- One team member reported our test emails were being delivered as “Junk” in his tests, so we performed additional testing.

Georgia Tech Spam Filters & Quarantine Protection

- **Spam Filters**
 - These are designed as the first line of defense to block unwanted marketing, phishing, and malware emails before they reach user inboxes
 - These also offer customizable settings: GA Tech IT admins can adjust filter sensitivity and whitelist trusted senders for optimal control.
 - Most also include machine learning to continuously learn from user and IT admin feedback and global trends to improve accuracy.
 - Based on test messages, we believe GA Tech is using O365 protections for this.
- **Quarantined Messages O365 leverages these options (which we observed during our testing)**
 - Safety Net: Holds suspicious emails for review before reaching your inbox.
 - Review & Release: Safely access quarantined emails if mistakenly flagged as spam.
 - Permanently Delete: Remove unwanted emails from quarantine to free up space.
- **AI-Powered Spam Detection: O365 leverages some of these capabilities, but we are unsure from the outside which options GA tech may be leveraging, so we performed extensive testing to ensure our email would pass spam filters**
 - Advanced Algorithms: Analyze email content, sender reputation, and behavior patterns for deeper insights.
 - Real-Time Adaptation: Continuously learns from new threats and adapts detection methods.
 - Phishing Protection: Identifies sophisticated phishing attempts using AI-based analysis.
 - AI based mail filters used by GT dynamically changing with learned domains.
- **What did we test?**
 - We need to ensure our message is not flagged as spam, quarantined, or detected.
 - First, we isolated messages that were not being flagged as “Unverified” or Spam and tested what emails did trigger the spam filter by sending emails to our GA email address from a number of sources.
 - We found that they quarantined unsolicited commercial messages we tested like “Eventbrite”, as well as some of our truly suspicious messages.

Spam filter woes



- In order to ensure the test phishing email would make it past spam filters, multiple email tests were conducted. These showed that email content with data entry were flagged by the filters, and the tool we initially proposed to use - GoPhish, was unsuccessful in email being delivered to the test victim inbox, likely due to known signatures of the tool.
- Well-known public email services or SMTP servers were also flagged by Outlook spam detection
- Email services used in our tests included locally running Mailhog/Postfix, att.net, gmail.com and fastmail.com.
- We selected Fastmail to deliver the exploit as it was the most believable option for which we had successful delivery and non-detection by GA tech email spam filter based on testing
- An attached PDF file was used to demonstrate the type of PDF with embedded malware we would have sent to the victim, as a true malicious actor.

The Phish Process

Message layout/formatting

- Full text of the email included in next slide, but generally designed a message to appeal to the target's emotions about being a veteran.

Plausible addressing

- The addressing considered for the Phishing email is from a believable domain like va.gov, gtri.gatech.edu. Given issues with the spam filter, we ultimately determined it was better to use fast mail as a believable domain in order to evade the spam filters and ensure our email ended up in the target's inbox.

Believable social engineering approach

- Using the background information we gathered during our research, we developed a believable approach designed to appeal to the target's emotions
- We explored using available tools like GoPhish, gmail, mailhog in order to determine the best approach

URL Obfuscation

URL obfuscation

- [Google sites](#) URL is used to demonstrate a fake phish website to solicit credentials or a CAPTCHA authentication illusion
- URLs are inserted in the phishing email to lure the victim to click the hyperlink
- Test landing page shows the sample rogue site



Sign in



Or create an account

- [Create an account with Login.gov](#)
- [Create an account with ID.me](#)

Phishing exploit used

Dear Mr. Michael Brown,

This letter is a summary of benefits you currently receive from the Department of Veterans Affairs (VA). Enclosed within this email, you will find an attached document that serves as an official record of your VA entitlement. It is imperative to safeguard this document, as it will play a crucial role in various applications and verification processes.

This official record has been specifically designed to assist Veterans, like yourself, in applying for a range of benefits. These benefits may include state or local property or vehicle tax relief, civil service preference, housing entitlements, free or reduced state park annual membership, and numerous other programs or entitlements that necessitate verification of VA benefits.

We understand the significance of your entitlements and are committed to ensuring that you have the necessary documentation to access the benefits you rightfully deserve. Please take the time to review the attached letter and keep it in a secure location for future reference.

If you have any questions or require further clarification regarding your VA benefits, our dedicated team is here to assist you. Please do not hesitate to contact our office at veterans@registrar.gatech.edu or visit our [website](#) here.

Thank you for your service, and we look forward to continuing to support you in accessing the benefits provided by the Department of Veterans Affairs.

Best regards,

David A. Ross, Ed.D
USAF Retired
Director, Veterans Resource Center
Phone: 404-385-2067
Email: dross35@gatech.edu



SummaryofVABenefits
Flyer.pdf



Thank You

Team 19
(Bryan, Megan, Ravi, Suraj)