TVACCU Phishing Simulation Proposal

James Palmer

December 2024

Executive Summary

This proposal outlines a free phishing simulation designed to evaluate TVACCU's resilience to phishing and provide training for its employees. It includes all of the open-source intelligence (OSINT) that has been collected about TVACCU and the phishing emails that could reasonably be created with that information.

The introduction emphasizes the prevalence of phishing attacks and the critical importance of being prepared for such attacks. If further action is approved, a follow-up proposal will be written that provides the technical details of the simulation's execution, including how the emails will be sent, how data will be collected and interpreted, and how that data will be reported.

By approving the phishing simulation detailed in this proposal, TVACCU can gauge its current ability to detect and prevent phishing as well as improve upon that ability to reduce the risk of a breach through a very common type of attack.

Contents

1 Introduction

Phishing is an ever-present information security issue that threatens all organizations, regardless of size. Egress's 2023 Email Security Risk Report surveyed 500 businesses that use the Microsoft 365 environment, and 92% of those surveyed were victims to phishing attacks in 2022. Of those who fell victim, 86% suffered negative consequences because of the attack. Additionally, 85% of malicious account take-overs the surveyed companies experienced began with a phishing email.

The FBI's 2023 Internet Crime Report shows that phishing is the single most common type of malicious activity that an entity may face. In fact, phishing made up the majority of reports of cyber crime reported to the FBI in 2023, with 298,878 cases total. The second most common category, personal data breaches, only had 55,851 reports filed. Figure 1 shows the number of reports filed with the FBI for common types of cyber crimes over the last 5 years.

Guarding against phishing should be a high priority for any organization, and it is doubly important when an organization handles a large amount of customers' personal information. Financial institutions are held to high standards in terms of information security, and such institutions may face heavy fines in the case of a data breach. Phishing poses a unique risk because of its abuse of human nature. No amount of technical controls can prevent every single phishing email from reaching an employee's email, which often makes the discretion of the recipient the deciding factor.

Phishing simulations are a proven method for both assessing an organization's resilience to phishing and training employees to more reliably discern what emails could be phishing attempts. The following sections detail how a phishing simulation could be carried out for TVA Community Credit Union.

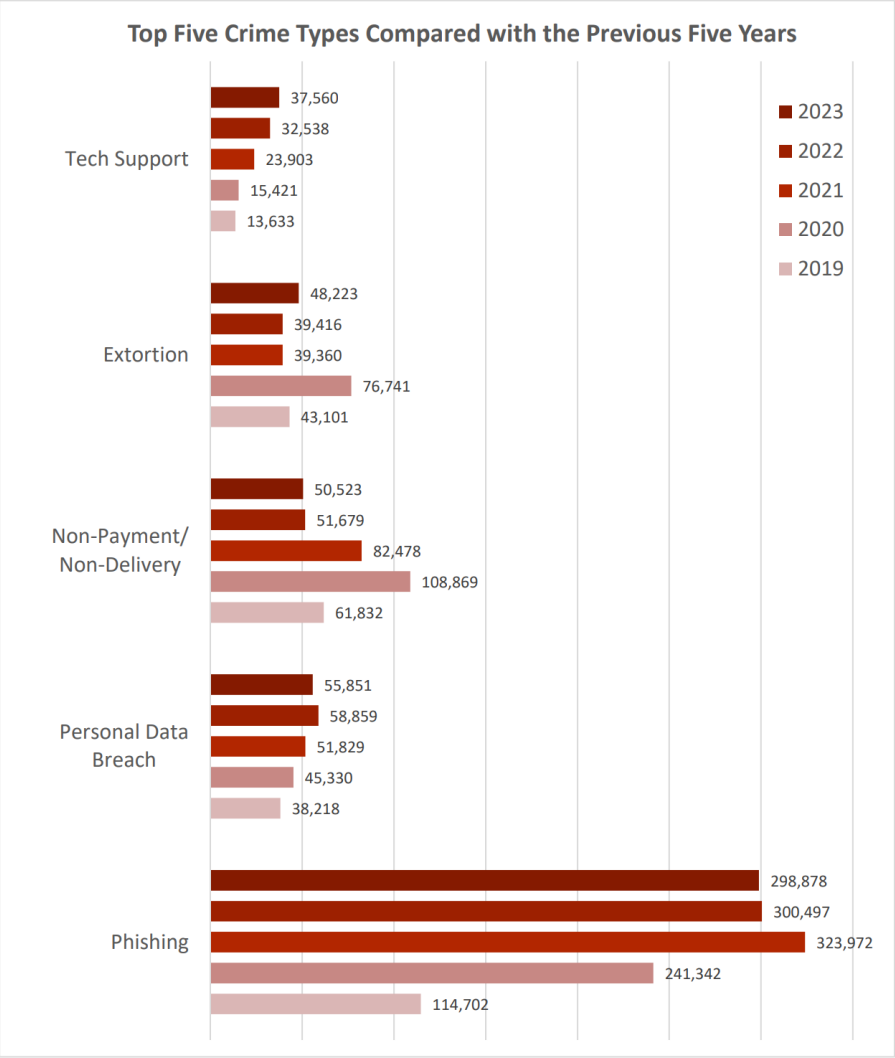

Figure 1: FBI 2023 Internet Crime Report - Graph of common crime types over the last 5 years

2 Open-Source Intelligence (OSINT)

The first step a malicious actor will take when preparing for a phishing attack will be to collect OSINT on the target. OSINT is information that can be freely gathered about the target from sources like the Internet and phone calls. OSINT in and of itself is not dangerous, but it may be used by attackers to plan their approach to interactions with their targets. The following sources were used to gather information about TVA Community Credit Union:

- TVACCU's Website - tvaccu.com
- LinkedIn
- Facebook
- Phone Calls

This list is very short, and that is intentional. While a wide variety of tools can be used, these three sources hold enough information to make enough pretexts for a small-scale simulation. The only information that may be used in any phishing attempt is information that can be proven true from the following sources. It is also important to note that the information collected cannot be proven to be completely accurate, and that is a risk that attackers are willing to accept when collecting OSINT.

2.1 TVACCU's Website - tvaccu.com

The target's own website will almost always be the first source of OSINT an attacker will utilize. The following sections describe the information gathered from tvaccu.com.

2.1.1 Phone Numbers & Email Addresses

The page *https://www.tvaccu.com/branch-locations/* provides addresses and phone numbers of each branch. The same webpage also lists the names and email addresses of each branch's manager. The page *https://www.tvaccu.com/find-a-loan-officer/* provides the names, email addresses, and phone numbers of loan officers.

The phone numbers can be used to collect further OSINT through phone calls. Additionally, they could be targets for vishing, a term for phone-based phishing attacks. The names and email addresses of branch managers could be incredibly useful for a variety of reasons. First, they already provide a list of emails that could be targeted for phishing without having to do much extra research. They also provide names that could be used in impersonation-based phishing, where the attacker poses as a fellow employee in a position of authority. Since the email addresses end in "@tvacuweb.com", it can be determined that tvacuweb.com is the domain that hosts TVACCU's mail client. An attacker could buy a similar domain like tvaccuweb.com or tuacuweb.com to attempt to trick employees into believing the email came from a fellow employee. Lastly, these email addresses provide a strong basis from which an attacker could guess the syntax of every employee's email. The emails found on tvaccu.com all follow the syntax of the employee's first name followed by a period and the employee's last initial or the employee's first initial followed directly by their last name. With just an employee's name, an attacker can reliably guess their work email address by sending their malicious email to addresses in both formats.

2.1.2 Mystery Shopper Program

The page *https://www.tvaccu.com/mysteryshopper/* details the Mystery Shopper Program that TVACCU uses to gauge the quality of the credit union's customer service. Customer-facing employees of TVACCU are likely to feel some level of anxiety about the Mystery Shopper Program, and an attacker could easily take advantage of that anxiety to convince an employee to interact with a malicious email.

Further credibility may be added to the phishing email by making it appear as if it came from the organization that provides the mystery shopper service. Clicking the "Register here" hyperlink on the same Mys-

ter Shopper Program page leads to a page that is owned by MemberXP: *https://www.memberxp.com/ms/?page=onlineapp*. Armed with the knowledge of the company that runs the Mystery Shopper Program, as well as a copy of their logo as provided on the registration page, an attacker could write a very convincing email that appears to be from MemberXP themselves.

2.1.3 Fiserv

By clicking the "Enroll" link on the page *https://www.tvaccu.com/online-banking/*, one may access an online banking enrollment page that displays the text "Copyright ©2024 Fiserv, Inc." This text provides a clue as to the company that owns the software that TVACCU uses. The page *https://www.tvaccu.com/card-console-privacy-policy/* also states that TVACCU's online banking is "powered by Fiserv". Therefore, it is safe to assume TVACCU uses a Fiserv product for account management.

2.1.4 Submitting an Application

The page *https://www.tvaccu.com/apply-for-employment/* provides another email address to contact: hr@tvacuweb.com. Additionally, a copy of the credit union's application form can be accessed from this page. An attacker could fill out an application with false information in order to add some legitimacy to a phishing email sent to hr@tvacuweb.com.

2.2 LinkedIn

LinkedIn can be used to find the names and positions of employees of TVACCU. Since the syntax of the organization's email addresses can be determined, this additional information can be used to send phishing emails to even more employees. For privacy's sake, no further information was collected about the people who have LinkedIn profiles associated with TVACCU. For brevity, the names and positions of every employee found on LinkedIn will not be listed here, but they can be found at *https://www.linkedin.com/company/tva-community-credit-union/people/*.

2.3 Facebook

Facebook is usually a valuable source of information about an organization. Since TVACCU is a smaller financial institution, there is less valuable information that could be utilized for phishing than one might expect. One piece of information that could be used in an attack is the following post: *https://www.facebook.com/share/p/2xdLJGb9UNNgCXH2/*. This post as of November 2024 has 103 comments, and the vast majority of them are rather emotional. The post itself is a complaint about TVACCU being closed during their transition to a new software product. This information can be used in conjunction with the knowledge that TVACCU currently uses a Fiserv product to conclude that TVACCU has only been using that given Fiserv product since the beginning of October. Since members seem to feel very strongly about the software change, it is likely that employees of TVACCU also have strong emotions (whether positive or negative) about the new software product. Strong emotions are a very good target for phishing attacks, so this information will be used when creating malicious emails.

2.4 Phone Calls

Since no actions have been approved yet, no phone calls have been performed to collect OSINT. If phone calls are to be performed, their purpose would be to confirm which Fiserv product TVACCU currently uses. If an attacker were able to determine exactly which Fiserv product TVACCU uses, the emails they create could be much more specific and therefore more likely to get a response. The phone numbers that could be called are those collected from tvaccu.com. Both approaches proposed in the following sections require impersonating an employee of another local credit union, like Florence Federal Credit Union or Valley Credit Union.

2.4.1 "Gossip" Approach

While impersonating an employee of a local credit union, the caller will mention that they are looking to change to a new software product. Additionally, the caller will state that members have mentioned that TVACCU recently changed to a new system. Alternatively, the caller can state that they saw on Facebook that TVACCU just changed to a new software product. The caller will then ask what product TVACCU now uses.

2.4.2 Software Shopping Approach

While impersonating an employee of a local credit union, the caller will mention that they have been tasked with calling other local credit unions to see what software system they use. The caller will mention that they saw on tvaccu.com that TVACCU uses a Fiserv product and that the caller's credit union is currently using Fiserv's Galaxy system. The caller will then ask what Fiserv product TVACCU uses.

3 Emails

With the information gathered from OSINT, an attacker will create a suite of malicious emails to send to his targets. The following sections describe the emails that could be created with the OSINT gathered about TVACCU and which type of employee would be targeted by each email.

3.1 Fiserv Representative Impersonation

Below is an example of an email that could be sent that aims to impersonate a Fiserv employee and could be used to target any employee:

> Hello `[Employee Name]`,
>
> Our records indicate that your organization, TVA Community Credit Union, has been using a new Fiserv product for a few months now. We at Fiserv care about customer satisfaction, so we have created a short survey that will enable you to provide feedback about your experience with our product.
>
> Please click the link below to take the survey:
> `[Hyperlink to phishing site]`
>
> Thank you,
> `[Fake Fiserv Employee Name]`
> `[Email signature inlcuding Fiserv logo]`

3.2 Mystery Shopper Program Results

Below is an example of an email that could target tellers by claiming to have results of a recent mystery shopper visit:

> `[Employee Name]`,
>
> You recently performed a transaction for a member who is part of the Mystery Shopper Program. Click the link below to view the feedback the member provided regarding their experience:
> `[Hyperlink to phishing site]`
>
> *Note: the above link will expire 7 days after receipt of this email.*
>
> MemberXP
> memberxphelpdesk@cusg.com
> `[MemberXP logo]`

3.3 Other Possible Emails

As mentioned earlier, an email containing a malicious link or attachment could be sent to hr@tvacuweb.com under the guise of a job application. This approach will not be used if further action is approved because it could needlessly punish an employee who processes legitimate job applications through email.

Another possible approach would be to target loan officers with emails inquiring about opening a loan through TVACCU. The email could contain a malicious link or attachment under the guise of loan information or other financial paperwork. This approach could even take place over a series of emails, with the malicious content being included after the loan officer and attacker had already exchanged a few messages to build rapport. This approach could be used if such action is requested.

4 Conclusion

Phishing is an ever-present threat, and preparing for phishing attacks is vital to maintaining security within an organization. Using only publicly

available information on the Internet, attackers can formulate a variety of malicious emails that may convince employees to divulge sensitive business or customer information. A phishing simulation performed at no cost to TVACCU could aid in determining the organization's current resilience to such attacks as well as provide training for employees, preparing them to detect malicious emails in the future. Upon approval of further action, a second proposal will be written explaining how the simulated attacks could be carried out. Additionally, a document containing all employee contact information gathered off of the Internet can be provided on request before the information is used in the proposed simulation.