No Phishing With the Wrong Bait: Reducing the Phishing Risk by Address Separation

Vincent Drury
Department of Computer Science
RWTH Aachen University
Aachen, Germany
drury@itsec.rwth-aachen.de

Ulrike Meyer
Department of Computer Science
RWTH Aachen University
Aachen, Germany
meyer@itsec.rwth-aachen.de

***Abstract*—Email-based phishing is still a widespread problem, that affects many users worldwide. Although many aspects of phishing have been extensively studied in the past, they mainly focus on the execution and prevention of different types of phishing and do not consider the process how attackers collect the contact information of potential victims. In this paper, we analyze the collection process of email addresses in more detail. Based on the results of this analysis, we propose email address separation as a way for users to detect phishing emails, and reason about its effectiveness against several typical types of phishing attacks. We find, that email address separation has the potential to greatly reduce the perceived authenticity of general phishing emails, that target a large amount of users, e.g., by impersonating a popular service and spreading malware or links to phishing websites. It is, however, not likely to prevent more sophisticated phishing attacks, that do not depend on the impersonation of a previously known organization or entity. Our results motivate further studies to analyze the usability and applicability of the proposed method, and to determine, whether address separation has additional positive effects on users' phishing awareness or automated phishing detection.**

1. Introduction

Phishing is still a serious problem for users worldwide [1], [2]. Whether it be used in mass phishing campaigns, that target many users in an automated fashion, or as entry points into organizations and communities in more sophisticated attacks, the phishing threat is still present and evolving.

To better understand attacks and methodically evaluate defenses, the research community has created several taxonomies and models that attempt to describe typical phishing attacks. These focus on the modeling process itself (e.g., [3]), or on overviews of attack types and defenses (e.g., [4]–[6]). In the first step in these models, attackers typically initiate wide-spread phishing attacks by contacting their victims. What these models miss, however, is the exact process of obtaining victims' contact information, e.g., their email addresses. In this paper, we provide an overview on the email collection techniques available to phishers. We derive these methods from the related problem of spam email, where the collection of addresses is better studied than for phishing. Although there are types of phishing attacks that do not use emails (e.g., SMiShing, Vishing [7]), we focus on email as the most prominent threat (96% of social attacks in data breaches in 2018 were performed via email [2]) and leave other types for future work.

Our analysis of the collection process indicates, that attackers are unlikely to gain the email addresses used to register at popular services. We therefore propose email address separation, where users explicitly separate email addresses they use to register at different legitimate services, thus preventing the leakage of an email address to attackers from affecting their other accounts. To reason about the expected effectiveness of address separation, we analyze usage and attack scenarios, with a closer look at email aliases, as they are typically easier to set up than different email accounts.

We find, that email address separation has the potential to greatly reduce the risk of general phishing attacks that impersonate known senders. It is, however, unlikely to offer much protection against some more advanced attacks.

The rest of this paper is structured as follows: The next section presents related work on email address collection and alias addresses. Section 3 introduces several techniques to achieve email address separation, and gives an overview of the support of these techniques by popular Email Service Providers (ESPs), as well as several typical email address usage scenarios. Section 4 takes a closer look at the email address collection process of attackers, and analyzes email address separation under several attack models. Finally, Section 5 presents a discussion on the proposed methods, including general problems and open questions.

2. Related Work

This work is concerned with the email address collection methods of malicious actors and the evaluation of email address separation techniques, specifically email aliases. These have been studied in different contexts before, which, in addition to an overview of existing methods for phishing prevention, are presented in this section.

Phishing Prevention There are several technical approaches to phishing detection and prevention. Popular

This research was supported by the research training group "Human Centered Systems Security" sponsored by the state of North-Rhine Westphalia.

DOI 10.1109/EuroSPW51379.2020.00093

methods include blacklists, which are integrated into most modern browsers but often leave a window of opportunity to attackers, as there is a delay between the creation of a phishing website and its first occurrence in the blacklist (e.g., [8]). To speed up the detection of unknown websites, numerous heuristic based approaches have been proposed, including approaches based on the body of a website (e.g., [9]), based on URLs (e.g., [10]) or based on emails (e.g., [11]). Though these systems are able to detect previously unknown phishing websites, they often suffer from higher false positive rates and are not currently integrated into popular browsers. Other works take a complementary approach and focus on stronger authentication mechanisms that can prevent phishing, e.g., U2F [12]. Though U2F has been deployed by several large websites, these methods are not yet widely available nor accepted by a large number of users.

The method proposed in this work provides detection capabilities that are orthogonal to existing approaches, thus enabling them to be used in combination.

Spam and Phishing Email Collection: The email collection process of spammers and other attackers has been studied to some extent in the past. Kreibich et al. take a closer look at the spam distribution process of the Storm Botnet [13]. They observe, that the botnet uses emails harvested from infected machines, as well as addresses scraped from the internet (website scraping). Shue et al. focus on website scraping, the effect of email address obfuscation and the differences of posting addresses on public and private websites [14]. Their findings indicate, that simple email obfuscation can deter spammers from using an address, and that addresses posted on public websites are likely to be used in spam campaigns after a short amount of time. In addition, they register accounts at several services and track, which email addresses receive spam messages. Here, none of the addresses used to register at popular websites received spam, but some of the addresses used for less popular websites did receive spam messages in a period of five months. Prince et al. also look at website scraping, and focus on the attributes and behavior of email address harvesters [15]. They compare fraud-based spam (e.g., Phishing) to typical product-based spam and find, that fraud-based messages are more likely to be sent shortly after an email address was harvested, and that email addresses are only used for few campaigns (as observed over a period of approximately eight months). They also find, that spammers and phishers both use website scraping to collect email addresses, which supports our assumption that the email collection techniques of spammers and phishers are similar. Polakis et al. approach the problem from an attacker perspective, and propose a method to use user names and nicknames harvested from social networks to brute-force possible email addresses [16]. The possible addresses are than fed to a search engine, and the results are parsed to extract email addresses. In this way, they are able to create a large corpus of possible email addresses, that can even be augmented with additional context information for targeted phishing attacks.

As these results focus on the collection of email addresses, they are used as input to our analysis in Section 4.

Alias Email Addresses: There have been several proposed email aliasing systems with different properties and goals. Ng et al. propose an alias system that can be used to trace email address leakage from different services and prevent spam [17]. Aliases can be set up via a central system, and users can retire an email address once it starts to receive spam. To argue about the usability of the system, they set up a prototype and offer it to students, 80.9% (n = 68) of which decide to use the system throughout the semester. In a second evaluation, they register accounts at 157 websites and track over a period of 15 days, which aliases receive messages from websites that are not affiliated with the original website. They notice, that some of the services do leak the email addresses to other providers, but also state so in their privacy policies. Similar systems are also proposed and analyzed by several other authors (e.g, [18], [19]). Kawashima et al. propose an aliasing system, that can be used to create and manage aliases to prevent spam and other types of malicious messages [20]. A tracking code encoded in the email address can be used to trace email address leakage. This system is taken up by Bose et al. in their phishing taxonomy, proposing to use it to trace the source of address leakage and preserve the identity of the end user [21]. They argue, that user effort to adopt such a system would be low, but that current adoption rates are low as well. They also identify the alias server as a single point of failure, and argue that aliases only provide limited protection against malware. They do not, however, take a closer look at usage and threat scenarios. In this work, we fill this gap by taking a detailed look at specific scenarios and arguing about the possible effectiveness of email aliases to not only trace address leakage but rather to prevent phishing in the first place.

3. Email Address Separation

Email addresses can be created not only by setting up new accounts, but also by extending existing accounts via aliases. Different techniques have different advantages and shortcomings, that we will discuss in the following. The techniques will also be further assessed in the context of usage and attack scenarios in Sections 3.3 and 4 respectively. We generally envision the following scenario for email address separation: A user Alice makes use of a number of services, e.g., `serviceA`, `serviceB`. She also creates a corresponding email address for each service, e.g., `address1` for `serviceA`, `address2` for `serviceB`. Suppose an attacker is able to compromise `serviceB` or otherwise obtain `address2`. Now, if the attacker were to use `address2` in a phishing attack impersonating `serviceA`, Alice would notice that the address does not match the service. In this way, she would be able to detect phishing attacks that do not use the correct email address.

3.1. Creating Email Addresses

Email address separation can be achieved in several ways. In this section, we present several approaches to creating and managing different email addresses.

Different Email Accounts: The strongest type of email address separation is creating several completely different email accounts. This offers a high level of separation and a lot of freedom in choosing different addresses, but requires a lot of overhead to manage. Though the overhead can be reduced by using email clients that can handle several accounts, the initial setup, where all accounts have to be created prior to subscribing to a service, cannot easily be reduced. Users will also have to handle a larger amount of accounts and credentials, which has the potential of overwhelming casual users, who even have problems creating unique passwords per account [22].

Full Alias: The next type of separation, called full alias, describes email accounts that offer users to freely choose alias email addresses in addition to their primary email address. The created address does not have anything in common with the original email address, but messages sent to an alias are received by the primary account. This has the advantage of completely separate addresses, while reducing the setup time and management overhead of using different accounts. However, there are also some inherent disadvantages to using aliases, as they offer less security once the primary account is compromised, which leaks all associated aliases and messages, and are restricted to addresses from one email service provider.

Tag-Based Alias: This type of address describes aliases, that can be created by appending a tag to the original email address. Examples include the "+"-tag based aliases used by Gmail, that allow users to add tags to their email address that will be routed to their original email account. The main difference to the full alias is, that the primary address can be deduced from any alias. It might also be possible, depending on the tagging scheme used, to infer the tag that was used for additional services from knowledge of the alias used for one service. An advantage of the tag-based approach is that tags do not have to be set up prior to registration at a new service, as all tags will be routed to the original address. This greatly reduces the setup and usage overhead of the previous methods. A disadvantage of the tag-based approach we observed by manual testing is that some service providers do not allow the use of the plus sign and other special characters in email addresses during account creation.

Others: There are several other possible approaches for users to separate their email addresses. A popular alternative, that is typically used to create accounts of low value are "throw-away" or one-time email addresses. These email addresses are often short-lived, and messages sent to them public, making them unsuitable for sensitive accounts [23]. Still, throw-away addresses are a possible way of extending existing separation types with an easy-to-setup alternative for low-value accounts. Another separation technique, that has been studied in the context of spam prevention, is the use of dedicated alias services (see Section 2). Here, users can sign up to the alias service with an existing email address and create aliases that are to be forwarded to this existing address. We will not discuss this latter type of alias separately, as it is just a flavor of the full alias type.

3.2. Alias capabilities of popular providers

To evaluate the feasibility of different email separation techniques, we looked at four popular email providers (Gmail [24], iCloud [25], Outlook [26] and Yahoo [27]). We determined which types of aliases these providers support by either creating an account directly and trying to create aliases, or referring to the online documentation of the service. The results (presented in Table 1) show that most of the large email providers offer some type of aliasing, though full aliases are usually restricted in number. This indicates, that the full alias separation approach is likely to still require several email accounts to separate a large number of services. Only one of the evaluated providers seems to currently offer a tag-based alias approach, making this approach harder to apply for users of other providers. The "Filtering" column indicates, whether the provider offers automatic filtering based on the offered alias technique in their web clients. Automated filtering can be used to visually separate emails in the inbox, easing the management effort for users. The last column indicates the stated purpose of aliases as advertised by the provider. It can be seen, that the purpose of full aliases is given as concealing the primary address for all providers in our list. One provider even explicitly states preventing the primary address from getting into the "hands of hackers" as a possible reason for using aliases. Apart from concealing the primary address, providers mention sorting and monitoring the usage of a specific email address as reasons to use aliases.

TABLE 1. ALIAS TYPES OFFERED BY POPULAR EMAIL PROVIDERS.

Provider	Full Alias	Tag Alias	Filtering	Purpose
Gmail	-	yes	yes	Sorting
iCloud	3	-	yes	Conceal+Monitor
Outlook	9	-	yes	Conceal+Prevent
Yahoo	1[a]	-	yes	Conceal

Numbers indicate restrictions on the possible amount of aliases in addition to the original address.

[a]Plus 10 send-only and 500 throwaway addresses.

3.3. Usage Scenarios

In addition to the different methods of creating email addresses, there are also several approaches to applying these addresses to enforce address separation. We analyze address usage from two different perspectives: The granularity of separation and the purpose of the address.

3.3.1. Address Separation Types. The granularity of the address separation affects the creation and maintenance overhead of the presented methods. In the following, we differentiate complete separation from security domains, where some services are grouped under a shared address.

Complete separation: Here, users choose a different email address for every service they use. This results in a large overhead when using different email accounts, as the accounts have to be created before registration can be completed. The full alias method creates less overhead, but still requires the creation of a new alias before registration. In fact, a full alias setup likely requires several accounts as well, due to the restriction on the allowed number of full aliases illustrated in Table 1.

This method has the highest degree of separation among the methods discussed in this section, but is also the most complicated to set up and maintain. The exception are tag based aliases, as registration at a service can be completed with a fresh tag, and the tag-handling process of the new address added retroactively.

Security Domains: This scenario imitates commonly used separation techniques (e.g., [28]) and requires users to define different security levels (or security domains), followed by the creation of one email address per domain. Many users already have several email addresses, and might already use them in a similar fashion. This technique reduces the setup cost of the complete separation method, but also reduces the granularity of control as compared to the previously mentioned method. However, it has been shown, that reputable services are less likely to leak email addresses to spammers [14]. As such, it might be reasonable to assume that this is also the case for phishing, and that high-security addresses are less likely to be known to attackers. The granularity of the security levels can be decided during the initial setup, and extended at any time by adding more email addresses.

3.3.2. Email Address Purposes. In addition to the separation types, we also define three different categories of purposes for email addresses, that describe the message flow between sender and recipient. If applicable, we present examples how they are used in private and business contexts.

Subscription: Used for most online services, this category describes a one-way communication from service to user. The email address is only used to receive information (e.g., verification requests, information, confirmations), never by the user to initiate contact. This category is well suited for email address separation, as services can be cleanly separated and handled without overlap. It is commonly used in both private and business settings (e.g., account at payment service or social media).

Closed-World Communication: This category describes a situation, where the user discloses an email address to a selected group of people. Examples include sharing an email address with friends and family in a private setting, or with a particular customer in a business setting, and does not exclude receiving messages from potentially unknown senders. Though complete separation is still possible in this setting, e.g., when the user only communicates over a single channel with a single entity, problems arise in more complex situations. Email forwarding, multiple receivers and CCs make using email separation while communicating with a group of entities, that also communicate among themselves, much more complicated. Though complete separation of groups of receivers might still be possible, the security-domains approach to address separation might also be an acceptable compromise. As long as the given address is only used for communication within the group, the user would be able to identify impersonation of entities that are not part of the group, which also includes impersonation of subscription services as described above.

Open-World Communication: In this category, email addresses are openly shared with the general public. This type of purpose is often seen in a business context, where organizations publish addresses, e.g., as contact information for potential customers. These accounts are expected to receive emails from unknown senders, opening up the possibility for attacks that are not based on impersonation of known senders. It is, however, still possible to separate these public accounts from any number of private accounts, which enables the detection of impersonation of senders associated with the private addresses.

4. Attack Models

This section presents several common email phishing attacks and assesses the effectiveness of email separation as mitigation strategy. We begin with an overview of the email address collection methods used in spamming, and transfer them to phishing, before analyzing a number of attacks in Section 4.2. Note that we do not include the compromise of an ESP in our attack model, as this would leak all information associated with all email addresses at this ESP. The only way in which email address separation could somewhat mitigate this threat is spreading email accounts across several ESPs.

4.1. Email Address Collection

In the following, we provide an overview of common spammers' techniques and transfer them to common phishing attacks. The categories presented here are based on a literature review of related work (see Section 2), as well as several explicit cases of phishing attacks. It should be noted that it is likely that attackers will use several types of collection methods, or even buy an existing collection. Though we aim to offer a broad variety of techniques that covers as many collection methods as possible, attackers might be able to acquire victim information in other ways.

Website Scraping: This is a well studied technique, where attackers crawl the Internet and look for email addresses [14], [15]. In other words, they are able to obtain (possibly obfuscated) email addresses as long as they are publicly posted on the Internet. Users, who do not disclose their email addresses on the Internet would therefore be safe from this type of collection strategy. The separation techniques proposed in Section 3 can all be used to create an address that can be publicly posted and is not associated with any other service. Thus, they can be used to prevent attackers from gaining information on addresses that are associated with other services, except for tag-based separation, which would leak the original email address. Still, if unique and unguessable tags are used for other important services, these addresses will not be accessible to attackers.

Data Leaks: After large data leaks, the email addresses of leaked accounts are often available to buyers on blackmarket forums [29], which also makes them available to phishers. There are several ways how the address could be leaked, including data breaches, being sold (e.g., to advertisers), or accidental leakage (e.g., through public mailing lists, abuse of recovery mechanisms, etc). Assuming, that reputable targets are less likely to leak data [14], we conclude that email separation has the potential to mitigate this attack, as only low security addresses become available to attackers, who are unable to gain the higher-security addresses that would be necessary to launch successful attacks. In the complete separation model, even the compromise of one or more high-security service does not affect any accounts on other high-security services. This is not the case for the security-domain approach, as successfully attacking one service will influence any other service sharing the same security domain.

Unfortunately, this type of collection is less well studied than the previous method, likely because it would require inserting addresses into datasets that are going to be leaked, which is hard to predict.

Dictionary Attacks: Attackers are able to create dictionaries of known names and words, and combine them to create a large list of possible email addresses, that can then be used in spam or phishing campaigns. Typical examples of easily guessable addresses are of the form `firstname.lastname@company`. This can, for example, be circumvented by choosing hard-to-guess email addresses. Therefore, all types of email separation would protect against this collection strategy, providing the created addresses are hard to guess for attackers.

Malware: Attackers can extract contact information like email addresses via malware. Some strains of malware have been known to harvest accessible email addresses and even email threads from infected machines, leaking not only personal accounts, but also the addresses of all contacts like friends, business partners or customers [30]. The extracted information can then be used immediately, to propagate the malware, or it can be used in subsequent attacks. This collection method is more complicated to mitigate, as it abuses the closed-world communication model (see Section 3.3). If the account information of an infected user is abused to send phishing emails, address separation does not help the receiving party in detecting malicious messages. As such, even though email separation might still protect against following phishing campaigns, once malware is able to infect the local machine and access email account information, all addresses should be considered compromised.

4.2. Attacks

For this section, we review common phishing attacks, and assess the expected detection effectiveness of email address separation. We begin with general phishing and continue with a number of selected attacks that exemplify situations where address separation is less effective.

4.2.1. General Phishing.

General Phishing, in the context of this work, describes phishing where the attacker is not aware of the specific recipients of the “bait”. Though attacks might be targeted, they are also automated, and the attacker does not interact with the victims directly. This category includes the most basic type of phishing, where attackers send messages to a large amount of possible victims (e.g. via email) to make them enter their credentials on a fake website or open a malicious attachment. The attacks are based on impersonation, either of a known public entity (e.g., popular banking service, online shop, company) or an unknown entity (e.g., copyright lawyer). Taking into account the email collection methods available to attackers, it is unlikely that attackers are able to obtain the addresses of services with high reputation. As long as users are able to separate the impersonated entity using address separation, they can thus protect themselves from such attacks, as the addresses obtained by an attacker are not associated with the impersonated target. As such, address separation has the potential to prevent phishing that impersonates a target that the user already interacted with, which particularly includes subscription based services.

4.2.2. Selected Attacks.

Here, we look at several specific phishing techniques to assess, whether email address separation can be used to mitigate the threat.

Public Addresses: Attackers can use official and public email addresses to initially contact their victim. There are several types of attacks that can follow this pattern, including attacks where attackers, pretending to be interested in job offers, send malware infected files to human resources divisions [31]. As the email addresses used in these attacks are public and expected to receive messages from unknown senders, it is unlikely that address separation would have an impact on attacks that do not rely on impersonation of a known sender.

Impersonation of ESPs: One part of an email address that cannot be hidden is the domain of the ESP. As such, any email address, once obtained, can be used in phishing attacks impersonating the email provider [5]. This can be somewhat mitigated by using full aliases, as it stands to reason that the ESP will use the main address to send information. Tag-based approaches and complete account separation, on the other hand, do not offer such protection and are therefore vulnerable to this kind of phishing.

Victim-Initiated Contact: In this type of phishing, attackers set up a website or profile and wait for users to initiate contact (e.g., typosquatting [32], seemingly benign services). Since contact is initiated by the victim, who actively chooses to share a specific email address, email separation does not directly help in this situation. Harvesting the email address to use in a different attack is, however, unlikely to work, as long as the targeted service is associated with a different email address.

To summarize, we found that there are several attacks against which address separation has the potential to defend. Especially the separation of subscription based services has the potential to reduce the risk of general phishing. Furthermore, there exist trade-offs of security and usability for full separation and security domains, as full separation can potentially protect against data leakage, even of services with high reputation. We observe a similar trade-off for different address creation types: creating different email accounts can even mitigate the compromise of an ESP, full aliases offer a balance between security and usability but might require additional accounts for large number of services, and tag-based systems require the least overhead to set up but may leak information to attackers that are able to obtain any one address.

5. Discussion

In the previous section, we found that it seems to be possible to reduce the risk of general phishing by using email separation techniques for subscription-based services. This is due to the fact, that attackers are less likely to obtain information about possible victims directly from the source (i.e., the services a user registers at). Instead, attackers rely on third party collections, which enables the use of email separation to effectively prevent mass phishing, as emails will not reach the correct address.

There are, however, additional problems and open questions associated with email separation, which we will discuss in this section.

5.1. Email Address Leakage

Email addresses are not usually supposed to be kept secret. In some cases, it might be necessary to share the email address if a service is to be used effectively. Also, organizations might not consider emails as sensitive as, e.g., banking information or passwords. Some websites offer account recovery mechanisms via email, that could leak (parts of) the email address associated with the account to active attackers.

This leads to an inherent problem of the proposed method: Once an email is leaked, it becomes necessary to contain the damage. Non-technical users, that do have problems recognizing phishing email, might put too much trust into the separation system, and actually end up more susceptible to phishing mail once the email address leaks. On the other hand, if only one address is leaked, this still prevents attackers from moving to other services a user might use, and users are still able to change the address or alias if a data leak becomes known. Additionally, address separation can be used in a layered approach, where the user is assisted by automated tools for phishing detection, that profit from the context information gained from separation of services, which puts a restriction on the expected benign emails.

5.2. General applicability

Assuming that the proposed method is effective, there are still some situations where email address separation is not applicable. For example, many organizations (e.g., universities) do not let users choose their addresses. This makes it possible to use dictionary attacks against their users, even including targeted information, like the name of the organization and user. In addition, address separation is applicable only to email in its current form. Attackers might shift to social media, SMiShing, Vishing or similar, where accounts might be much harder to separate.

5.3. Usability

To make email address separation commonly usable, we argue that some usability requirements should be addressed. First, the creation process of different email addresses (accounts or aliases) should be as easy as possible to reduce the overhead of using address separation in the first place. This could be solved locally (e.g. by offering tools to generate fresh email accounts and aliases on a user's device) or supported by ESPs. The separation should also be supported by email clients, making it possible to sort and label emails according to different aliases or services. We could also imagine a tool that behaves like an (integrated) password manager, that can be used to comfortably generate and manage large numbers of email addresses. It might even be possible to add automated phishing email detection capabilities to the user's inbox, that can benefit from the context information given by separate email addresses. Lastly, changing an email address after data leakage should be possible and convenient. Users should be able to change their addresses once they are informed that the associated email address was leaked, to prevent attackers from using it in subsequent attacks. We plan to investigate the general user experience of address separation with a prototype implementation in the future.

5.4. Awareness

Lastly, a possible benefit of email separation is user awareness. It stands to reason, that users are more aware of the use of their email addresses if they actively think about separating them. This might increase their suspicion towards unknown senders in general, especially if they receive emails on an unexpected address. Consequently, this awareness might, for example, have an effect on phishing that uses an authority like the local police or a lawyer to attack users, as they might question how such an authority would have access to a particular email address.

6. Conclusion

In this paper, we analyze email account separation as a possible approach to prevent phishing. Attackers are rarely able to obtain their victims' email addresses directly from the service they are trying to impersonate, which makes it possible for users to recognize phishing by using separate email addresses for different services. We define several address separation usage scenarios, and argue about their usability and effectiveness. We present attack models, and find that address separation is most effective in the case of general phishing. For more advanced types of phishing, email separation might reduce the risk of follow-up attacks, but is likely far less effective than in the general case. We additionally discuss several problems that might arise when using address separation in a real-world setting.

For future work, we intend to create a prototype implementation of an email account management tool, that can be used to evaluate the real-world applicability of the proposed address separation method, whether a positive effect in user awareness can be observed, and whether the additional context information given by address separation can be used to improve automated detection of phishing emails.

References

[1] M. Vergelis, T. Sidorina, and T. Shcherbakova, "Spam and phishing in q3 2019," https://securelist.com/spam-report-q3-2019/95177/, accessed February 27, 2020.

[2] Verizon, "2018 data breach investigations report," https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf, accessed February 27, 2020.

[3] M. Jakobsson, "Modeling and preventing phishing attacks," in *Proceedings of the 9th International Conference on Financial Cryptography and Data Security (FC)*, 2005.

[4] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Computers & Security*, vol. 68, pp. 160–196, 2017.

[5] B. B. Gupta, N. A. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, 2018.

[6] G. Ollmann, "The phishing guide - understanding & preventing phishing attacks," 2004, White Paper.

[7] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: An assessment of threats against mobile devices," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, 2014.

[8] X. Han, N. Kheir, and D. Balzarotti, "Phisheye: Live monitoring of sandboxed phishing kits," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[9] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites," in *Proceedings of the 16th international conference on World Wide Web*, 2007.

[10] A. Blum, B. Wardman, T. Solorio, and G. Warner, "Lexical feature based phishing URL detection using online learning," in *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security*, 2010.

[11] A. A. Akinyelu and A. O. Adewumi, "Classification of phishing email using random forest machine learning technique," *Journal of Applied Mathematics*, vol. 2014, 2014.

[12] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor a two-phase usability study of the fido U2F security key," in *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[13] C. Kreibich, C. Kanich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamcraft: An inside look at spam campaign orchestration." in *Proceedings of the 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2009.

[14] C. A. Shue, M. Gupta, C. H. Kong, J. T. Lubia, and A. S. Yuksel, "Spamology: A study of spam origins," in *Proceedings of the 6th Conference on Email and Anti-Spam (CEAS)*, 2009.

[15] M. B. Prince, L. Holloway, E. Langheinrich, B. M. Dahl, and A. M. Keller, "Understanding how spammers steal your e-mail address: An analysis of the first six months of data from Project Honey Pot." in *Proceedings of the 2nd Conference on Email and Anti-Spam (CEAS)*, 2005.

[16] I. Polakis, G. Kontaxis, S. Antonatos, E. Gessiou, T. Petsas, and E. P. Markatos, "Using social networks to harvest email addresses," in *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES)*, 2010.

[17] B. H. Ng, A. Crowell, and A. Prakash, "Adaptive semi-private email aliases," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2012.

[18] D. Mazieres and M. F. Kaashoek, "The design, implementation and operation of an email pseudonym server," in *Proceedings of the 5th ACM Conference on Computer and Communications Security*, 1998.

[19] J.-M. Seigneur and C. D. Jensen, "Privacy recovery with disposable email addresses," *IEEE Security & Privacy*, vol. 1, no. 6, pp. 35–39, 2003.

[20] M. Kawashima, T. Abe, S. Minamoto, and T. Nakagawa, "Cryptographic alias e-mail addresses for privacy enforcement in business outsourcing," in *Proceedings of the 2005 workshop on Digital identity management (DIM)*, 2005.

[21] I. Bose and A. C. M. Leung, "Unveiling the mask of phishing: Threats, preventive measures, and responsibilities," *Communications of the Association for Information Systems*, vol. 19, no. 24, pp. 544–566, 2007.

[22] E. Stobert and R. Biddle, "The password life cycle: User behaviour in managing passwords," in *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*, 2014.

[23] H. Hu, P. Peng, and G. Wang, "Characterizing pixel tracking through the lens of disposable email services," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (S&P)*, 2019.

[24] Gmail Help, "Send emails from a different address or alias," https://support.google.com/mail/answer/22370, accessed February 27, 2020.

[25] iCloud User Guide, "Use email aliases on iCloud.com," https://support.apple.com/guide/icloud/use-email-aliases-mm6b1a490a/icloud, accessed February 27, 2020.

[26] Outlook Support, "Add or remove an email alias in outlook.com," https://support.office.com/en-us/article/Add-or-remove-an-email-alias-in-Outlook-com-459b1989-356d-40fa-a689-8f285b13f1f2, accessed February 27, 2020.

[27] Yahoo Safety Center, "Your Yahoo ID and aliases," https://safety.yahoo.com/Privacy-Identity/YAHOOID_AND_ALIASES.html, accessed February 27, 2020.

[28] J. Rutkowska, "Partitioning my digital life into security domains," https://blog.invisiblethings.org/2011/03/13/partitioning-my-digital-life-into.html, accessed February 27, 2020.

[29] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware? Understanding the risks of stolen credentials," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (CCS)*, 2017.

[30] SophosLabs Research Team, "Emotet exposed: looking inside highly destructive malware," *Network Security*, vol. 2019, no. 6, pp. 6–11, 2019.

[31] Malwarebytes Labs, "Petya- taking ransomware to the low level," https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/, 2016, accessed February 27, 2020.

[32] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The long "taile" of typosquatting domain names," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security)*, 2014.