Unawareness of Leaking Private Data

Jian Wang
Computer Science
SUNY Binghamton
Binghamton, NY 13902, USA
jwang375@binghamton.edu

Ethan Ferguson
Computer Science
SUNY Binghamton
Binghamton, NY 13902, USA
efergus3@binghamton.edu

***Abstract*—People's privacy is always leaked unconsciously, no matter whether the person who collects other people's information is intentional or unintentional. There are two methods of collecting private information of others, technical and non-technical. At the same time, the emerging discipline of social engineering has also summarized various methods of spying on other people's privacy. After analyzing some typical cases of privacy data leakage and summarizing some privacy data theft methods, this paper will put forward some suggestions for privacy data protection. These recommendations are still based on the discipline of social engineering.**

***Keywords*—Data Privacy, Social Engineering, Attacking, Data Leaking**

I. INTRODUCTION

People always inadvertently leak various personal information in their lives. Even in a casual conversation, a person's habitual words and tone of voice can always give away the narrator's age range. When the Internet has flooded people's lives, various social media have exposed people's personal lives to the fullest. As described in the book "Social Engineering: The Science of Human Hacking"[1]: In the last century, if I peeked at my sister's diary, I would probably be beaten half to death by my sister; But now, she would be frustrated that no one reads her daily updates. It is not correct to say that people are deliberately revealing personal privacy by posting social platform dynamics. Because the expectation of most people is to only share these life bits with their friends and always think that their "friends" have goodwill towards them, and they will not maliciously spy beyond the boundaries they think. But in essence, other people's hearts are incalculable and beyond your control. In many cases, the leakage of privacy begins with the gossip of close friends. A store sign that you inadvertently photograph can give away your current location, even though you didn't mention your current location or label your location. Sometimes, there are still some people who are not close to you in your social software friend list, and even some business partners don't know your age and surname. But when you post pictures of a birthday party, the candles on the cake can give away your age, and the cards your friends write to you can give away your full name. These are times when you may not care about it, but inadvertently reveal your personal privacy. The above example only reveals some unimportant information. Sometimes, an irresponsible service provider may leak important information such as your driver's license, but you are not aware of the potential danger.

As mentioned in the paper "Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses": employee education can better prevent social engineering attacks. More public cases of personal privacy information leakage and the popularization of privacy protection methods will help the public resist theft and attacks on personal privacy. Although we will never be able to eliminate privacy leaks because people are very subjective, educated people may not be able to implement privacy protection as required for various reasons, and attackers will continue to improve their attack skills, we can at least reduce privacy leaks frequency of cases. Most of the content of social engineering is related to this, so this article focuses on privacy theft and targeted privacy protection in social engineering and provides readers with practical suggestions for reference and study.

II. BACKGROUND

The issue of privacy leakage is not a recent issue. On the contrary, it has always been a hot topic since the birth of an ancient social platform like BBS. In order to prevent privacy leaks, people always make various efforts at technical and non-technical levels, but there are endless cases of privacy leaks that cannot be prevented. Just as WeChat can quickly make friends through the function of nearby people, there are many online dating software, such as Blued and Tinder, which also have similar functions. When users use software for making friends based on location information, location information is also directly leaked out. Jian once did an experiment when he was an undergraduate student. Jian used Blued to scan every hour in my lab on Tuesdays. As a result, almost all the single gay students and teachers in the school were swept out, because every Tuesday all the

[1] Nina Klimburg-Witjes and Alexander Wentland, "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," Science, Technology, & Human Values 46, no. 6 (October 2021): pp. 1316-1339, https://doi.org/10.1177/0162243921992844.

teachers will come to the school to start the week. Yes, all students will also be brought together for politics classes. They don't realize JIAN did it on purpose. The school Jian was in is not big, basically, Jian can tell who the owner of the account is by just looking at the dynamics they post on this dating app; even if Jian does not know, Jian can mosaic some of the information. Take it to ask friends around you, so you can quickly know who the owner of the account is. The method Jian uses is at the bottom of the social engineering pyramid: the "OSINT" information-gathering method. In this small case, Jian did not use any technical means to collect their information. The only feed Jian have is that single gay men liked or even preferred to use Blued to meet each other at the time.

Therefore, it is even more necessary for us to understand where social engineering is exploited.

According to the definition of Kaspersky, a world-renowned security vendor, social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.[2] In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. We can understand that the original intention of social engineering is to attack people. But social engineering master Christopher Hadnagy summarized these technologies and taught people a lot of ways to prevent social engineering attacks and organized this knowledge in a series of books he wrote. The social engineering pyramid consists of five layers. Its structure and content are shown in the figure below. They are OSINT, Pretext Development, Attack Plan, Attack Launch, and Reporting.

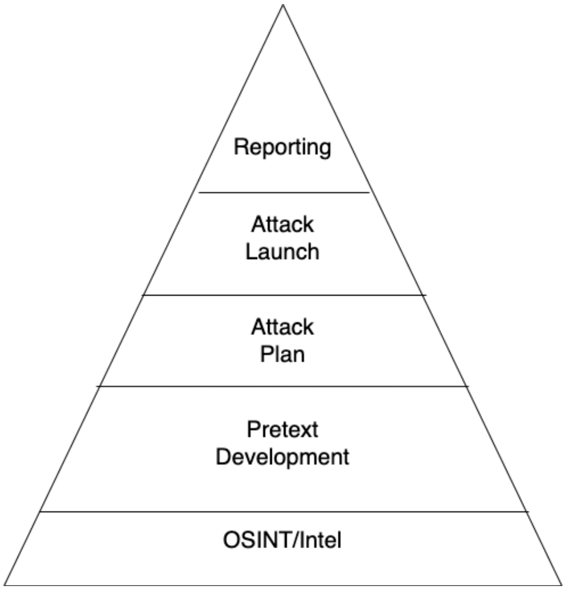

Figure 1 Social Engineering Pyramid

Since this paper focuses on the issue of privacy leakage, only the OSINT part will be discussed more in the paper. If readers want to understand this pyramid more deeply, please study "Social Engineering: The Science of Human Hacking" carefully.

III.CASE AND ANALYSIS

According to Oxford Dictionary, Privacy is the state or condition of being free from being observed or disturbed by other people. This article will not discuss all topics related to personal privacy, because this will make the article too long, but it will discuss some daily office scenarios and situations that can always be encountered in personal daily life.

A. *Start with the name on the badge*

This is an example written by Christopher in "Social Engineering: The Science of Human Hacking", and it is also an example that Jian thinks is very representative. Jian has the corporate experience and now owns a company in New York. Jian has always disliked wearing a work ID at work because it would make it easy for any visitor to see his basic information. The example discussed next is a good example of why his concerns are justified.

In this example, Christopher was posing as a bidder with the goal of gaining access to the mailroom of a large medical facility. They carefully observed the security staff at work and the gates where staff congregated to smoke. He memorized the names of the security personnel, blended into the crowd, sneaked into the building, and when the duty officer in the mail room wanted to ask the security personnel for confirmation, he actively reported the name of the security personnel he had memorized, thereby preventing the duty personnel from calling the security personnel for confirmation, and then Successfully entered the mailroom.

From this example, we can see that because of the badge on the chest of the security personnel, when Christopher met him for the first time, although he failed to sneak into the company, he firmly remembered his name. This also created perfect conditions for him to sneak into the mail room later. When the person on duty in the mailroom made a request for verification, because he could correctly name the security personnel, the person on duty chose to believe him. And the cause of all this comes from the badge on the chest of the security personnel.

While we can't stop attackers from attacking others all the time, we can do everything we can to prevent ourselves from being attacked. Come back and analyze this case for more details. If the security personnel did not wear a badge, then Christopher would not ably know the

[2] Kaspersky Lab, “What Is Social Engineering?,” usa.kaspersky.com (AO Kaspersky Lab, September 8, 2022), https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

name of the security personnel, so he would not be able to convince the duty personnel to trust him, because the smooth reporting of other people's names will always give people a feeling that the speaker and the person being called know each other. And the duty officer in the mail room also had serious work negligence. Although Christopher reported the name of the security personnel, Christopher is a stranger after all. When confronted with an unfamiliar face, the duty officer should reconfirm the identity of the person with the security personnel. However, he did not fulfill his duty. Although it is a good virtue not to judge others with malice, it is also easy to be exploited by malicious attackers.

B. *Password Notebook and Password Label On Device*

This case does not come from a social engineering series, but from the personal experience of the author of this article, Jian, and the work experience described by his undergraduate cryptography professor.

As a co-worker of the Binghamton Chinese Church, Jian often provides free technical support on computers to the Chinese in the community. An old painter who was served has a habit like many others. Since the woman is old, has a bad memory, and has multiple sets of passwords for different accounts, she uses a notebook to record her various account numbers and passwords. Once when Jian went to her house to set up her new iPhone, she couldn't log in to her Apple ID because she couldn't find her password notebook. She wanted to reset the password, but because the Gmail email password used to set up the Apple ID was also recorded in the password book, the link to reset the password could not be accessed. At this time, because her mobile phone card was undergoing number portability, she could not receive the verification text message from Apple. As a result, the scheduled time for migrating mobile phone data was used to find the password book. When Jian asked her why she had to set up separate passwords for each account on different websites and always browse websites in incognito mode, she replied: "A computer student once told me that this is the only way to be safe!" So, when looking for the password notebook, and after finding password notebook, Jian had to re-educate her information security-related knowledge.

If that's one extreme, the example described by Jian's information security professor is on the other extreme side. Jian's professor was once invited by the Secrecy Bureau of a certain city in China to conduct a security inspection for them. As a result, when she walked into the office, the first thing she saw was the user login password pasted on the monitor. And at that time, all computers in the Security Bureau still used the Windows operating system and directly used the Administrator account, and pirated operating systems were prevalent.

While neither Jian nor his professors were attacking others in the above two examples, it would be easy for them to socially engineer the owner of the device in both examples at this point. If Jian took the codebook with him when he left, all the painter's accounts could be accessed at will, even if she "protected" them with different passwords. Also, the woman can't remember any passwords, so she can't log in to verify her identity when any account sends a warning email to her mailbox. Jian lived in the same small town as the woman and used the home broadband network provided by the same broadband provider, so some platforms did not feel that Jian's login behavior was abnormal. In the example Jian's professor recounts, the Secret Service employees represent the other extreme. They also couldn't remember the password, because the management conditions of the Bureau of Secrets required the strength of the password of the computer account, so they directly pasted the password on the bottom of the computer screen to save trouble. Although they won't have to worry about not being able to find the password notebook this time, it also makes it possible for anyone passing by to see their passwords. If the person entering the Secrecy Bureau is not Jian's professor but an agent, no matter how many and strong their passwords are, the trained agents can basically remember them. Even if they only need to remember the password of one of the computers, they can invade the entire office network through this one computer.

Although using multiple sets of different passwords helps to protect the security of each account, the premise of achieving this must also require users to remember these passwords. There is an interesting ad in Chrome, the main idea of which is shown in the picture below. Chrome saves all passwords for the user in a syncable Google Account. When a user uses Chrome to log in to the same Google Account on different devices, Chrome will automatically fill in the account and password for it. In fact, at this time, the combination of Google Account and Chrome is like an old painter's password notebook. If the user does not enable the two-factor authentication function for Google Account and uses the automatic password storage function of Chrome, then the attacker who obtains the user's password is like obtaining the user's password notebook. The principle of the attack is the same at this time. The password notebook can be regarded as the password shared by all accounts, because no matter which accounts the old artist wants to log in to, she must check this notebook first, and all account passwords are recorded in this notebook. So, in principle, the old painter only used one password for all accounts, and that was this notebook. If you can't understand this sentence, please bring this sentence into the Chrome example. Although it looks like you're using different passwords for different accounts, even if you're using Chrome's automatic strong key generation feature, these passwords are stored in the same account, and there is only one password for this account. If another Chrome is used to log in to the account that stores all passwords, all passwords can be recalled directly.

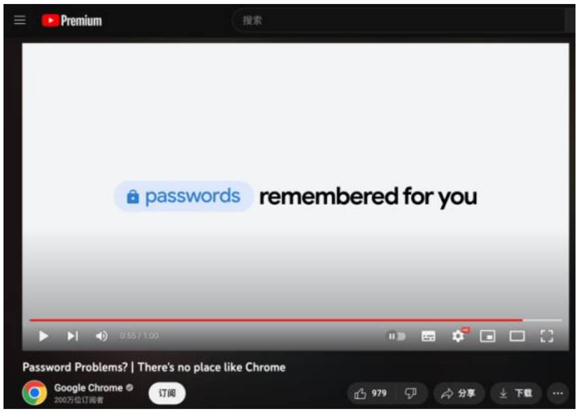
Premium
搜索
passwords remembered for you
0:55 / 1:00
Password Problems? | There's no place like Chrome
Google Chrome
200万位订阅者
订阅
979
分享
下载

Figure 2 Chrome "Password" Advertisement

Strong password policies don't apply everywhere. This has a lot to do with the scenarios in which it is applied. Highly sensitive government secrets probably don't want to use repeated passwords, and would perhaps store the password in a vault. But this does not mean that the civilian market is the same as the government. If the user cannot meet the basic requirement of remembering the password, then all the conclusions derived under this policy will be invalid. In the end, Jian's advice to the old painter was to use a limited number of passwords for all accounts, although there will be many accounts with repeated passwords. At least in this way, the woman no longer needs a notebook to record the password, and the new password is strong enough to resist brute force attacks in most cases. Security protection cannot be 100% successful and reliable. But if in most cases, a defense strategy is effective, then this defense strategy is also successful. Jian's professor also asked all staff to remove the password stickers on the screen.

Of course, the fact that you could be arrested for a crime you posted online is not an issue for most law-abiding citizens. However, the criminals posting online are just newsworthy stories that show people are overconfident and unaware, and that causes people to leak private data on the internet habitually.

C. Third-Party Websites

There are myriad ways people leak their private data without realizing it, and that often comes through interacting with third parties which either intentionally or unintentionally leak their data. The simplest case is on social media, where a person can post information they do not realize is sensitive. This has happened many times, and can leak lots of information. Facebook alone has had several important data breaches, with one in April 2021 leaking 530 Million Users' personal information including names and phone numbers [Heilgenstein]. This information was all publicly available at the time it was acquired (2019) and could have been accessed by anyone, although the manner of access was a bug. The attacker's exploited the ability to find friends by phone number to connect user accounts to other information. Even access to common identifiers like names and phone numbers is still useful to an attacker, who might use these for a phishing attack, and could do something more sinister.

One unexpected loss of privacy from social media comes in the form of people posting on social media or otherwise on the internet in an overconfident manner. Sometimes this is with the delibrate intention of leaking their own private information to prove a point, and other times it is because a user does not realize their private information can and will be accessed by anyone, even if they do not want them to if it is available publicly online. This happened in a very high-profile manner when the CEO of LifeLock posted his actual SSN, 457-55-5462, on the Internet. He did this to prove his confidence in the LifeLock product. Unfortunately, it showed their incompetence because his identity was stolen several times without him knowing, and he only found out years or months later because of debt collection agencies and similar contacting him [Zetter]. A similar case happened in 2014 when someone posted their actual passwords on the *Washington Post* website. Unsurprisingly, this resulted in many of their accounts being compromised [Fincher]. He did this as a response to the heartbleed vulnerability, to prove people were overreacting. Instead, he only proved his own incompetence. This type of behavior happens frequently with people commit crimes. I know I have seen many people post their own illegal activity on the internet (drinking underage, doing illicit drugs, shoplifting) and it is reported that this happens somewhat frequently, although actual statistics are difficult to find. Law enforcement has certainly been known to use social media posts to find criminals who posted their activity on the internet, and the act of posting crime on social media even has a name: "performance crime" [Surette]. Police using social media can be especially effective for catching crimes like shoplifting, where a criminal may post records of their stolen goods online. Small crimes like these are common in performance crime because of how low-level and common they are, and the perpetrator does not believe they will be caught. However, they sometimes are. In one example of this, an Illinois woman was arrested after she posted a photo of herself in a distinctive dress and even made it her Facebook profile picture [Moran]. In another instance, a boy bragged about getting a school shut down after posting on social media. The account he used was anonymous, but it was eventually traced back to him. It took police three months to finally arrest him, but eventually they were able to because of his boasting [Markowitz]. There are plenty of examples of performance crime leading to arrests if you go looking. Of course, most people know that if they post something publicly online it can be used against them in theory, but most people are also overconfident and do not believe it will happen to them.

Using trusted software can also lead to data breaches in a more intentional manner. Intentional, that is, to the companies leaking the data because they are being paid for it. This happened recently with several tax filing websites which were found to be sending user's data to Facebook in November 2022. This data included very sensitive information like names, email addresses, users' income, filing status, refund amounts, and dependents' college scholarship amounts, and more [Fondrie-Teitler et al.]. Similar data was also sent to Google, although anonymized, but simple anonymization has been shown to be an insufficient way to protect privacy and has been a topic of study for decades. Tax software would generally be considered incredibly sensitive, so the fact that even they are sending detailed information to Facebook and other tech conglomerates should be seen as incredibly concerning. Where your data is sent by the companies you give it to is almost impossible to know and giving out information to anyone should be treated with utmost caution. Even when there is no data breach, your data can be sent to companies all over the world the moment you give it out, even by those you trust.

D. *Curiosity Killed The Catphished*

Many social engineering attacks exploit people's curiosity to get past security measures. This is especially useful when an attacker is targeting air-gapped or otherwise highly secure environments, where sending an email will be impossible or insufficient to compromise a system. Attacks that do this almost seem to be too good to be true. They do not require sending a suspicious email or directly interacting with the victim at all. All that is required for many of these attacks is to leave malicious USB sticks in the general vicinity of the targeted organization, and it turns out that repeatedly users will plug in the devices to see what they contain, often opening files and compromising their systems, which run on the company network. This has even been the course of action taken in high-profile international cyber warfare operations, notably being the vector used by the Stuxnet virus [Zetter, 2014].

One especially interesting case study which shows this attack in action is presented by Hadnagy and Fincher. Hired as security consultants for a company, they dropped a USB device containing a PDF file named "EmployeeBonuses.pdf" which would phone home if opened and used metasploit (A popular pentesting toolkit) to create a reverse shell on the target computer. Only a short while after planting the device, they had seven shells on the target's network! How could this be if they only dropped one device? Well, it turns out that people's curiosity got the best of them. Naturally, an employee of a company would be very curious to see what is on a pdf called "EmployeeBonuses.pdf", and because they were not aware that a USB device could be an attack vector and because any apprehension they had was overcome by curiosity, they attempted to open the file. Because the PDF was malicious, it would crash when opened, infecting the machine. Still wanting to find out what was on the device and still being unaware that this was suspicious behavior, the employees continued bringing the device to their friends until a total of 7 devices were infected [Hadnagy and Fincher]! As a result, an attacker using a technique like this could get any data on the target's computer or potentially escalate privilege to other computers on the network and steal other data.

This technique has not only been used in benign penetration tests, it has also been seen in "the wild" so to speak. In fact, at least one well known cyberattack used this technique. The worm in this attack is known as Stuxnet. Unlike most cyberattacks, which are financially motivated [Verizon], this worm was intended to damage Iranian nuclear infrastructure. The worm was first discovered in 2010 [Baezner]. The intention of the worm was to cripple the centrifuges used for uranium refinement in Iran, which the United States was concerned were being used for production of nuclear warheads. At least, this is the believed perpetrator and motivation. Getting a worm onto the devices in charge of controlling the centrifuges was an exceedingly challenging task because of the security of the facility. The computers in the Natanz nuclear plant were air-gapped, in their own isolated environment [Baezner]. As described before, it would be impossible to send a phishing email to get onto these devices, since the devices are not connected to the network the email is opened on.

Anecdotal evidence seems to support the idea that people are unaware of the fact that plugging in a random USB device potentially opens them up to many kinds of attacks but does not tell us how effective such an attack really is. As it turns out, it is quite likely that a random person will plug in and look at files on a USB stick they find [Tischer]. Tischer et al conducted an experiment at the University of Illinois where they left almost 300 USB drives around the campus and found that 45-98% of drives were plugged in, depending on location. This shows that people really are very unaware of the potential danger of connecting unknown hardware to their computer, and especially of opening files found on such hardware. They tracked users by putting html files with <img> tags directed at a traceable address to determine whether a usb drive was plugged in and a file opened. This is also a technique an attacker could use in order to get some information about a person without even having to develop an exploit, and could leak some data like user location. Of course, a truly malicious attack could get much worse and perhaps access all data on an infected computer. The reasons people reported plugging in the devices matched what we would expect of many social engineering attacks, they did it out of kindness and curiosity. Some said they wanted to find out who to return the device to. Others were simply curious what was on it. We find in many scenarios that people's natural tendency to be kind is, while nice, something which leads them to lose privacy unintentionally. Naturally, the systems these devices were plugged into were obviously not air-gapped, which would make it possible for an attacker to exfiltrate data [Tischer].

Despite its effectiveness, on an air-gapped network this technique has limited utility when it comes to leaking data. This is of course because in order to leak the data, it needs to be exfiltrated. There is a wealth of research on using techniques like side channel vulnerabilities to do such exfiltration, but if your goal is to protect data like government secrets, or even your personal information like social security number, an air-gapped network will be rather effective. If the network containing the data is compromised, it is possible the data could be destroyed, but it would be very difficult for an attacker to actually get ahold of the data.

In terms of actual usage, it seems enticing a curious victim to insert a malicious physical device is less common than remote attacks, but still a very popular technique. According to Proofpoint’s 2021 State of the Phish, a full 54% of organizations faced attempts of USB-Drop-based attacks in 2020, including 80% of United States organizations. Yet, this is something that is anecdotally not focused on very much in security training and security awareness at large. Given the severity of the success of such an attack, it is imperative that organizations take care in order to avoid succumbing to it.

IV. Another View

Yes, we should emphasize security and privacy all the time, but sometimes we overdo it.

A. *If Security Causes Inconvenience*

Anyone who has used some devices for high-secret systems knows that device authentication is very complicated, requiring USB Key or other biometric identification devices and high-strength passwords to be authenticated to log in. Now some systems used by the public are also moving towards such a password policy. Taking MacBook as an example, if the user has already entered the fingerprint, the user should not be asked for the password. But every time after restarting the computer, and accessing some system services, the authentication system of Mac OS always asks the user for a password. It is not a technical problem to use the fingerprint to log in after booting, because the face recognition and fingerprint recognition of Windows Hello can be used directly to log in to the user account when it is turned on for the first time, whether it is an administrator user or an ordinary user. If the user can already provide fingerprints and the possibility of forging fingerprints is extremely low, the user who applies for login at this time should be regarded as the account owner. If a person stood behind the owner of this Mac with a gun and forced him to unlock and hand over the data, neither fingerprints nor passwords could stop the data, or it would be taken away. So, at least for mass users, security is a decision that needs to be balanced. Sometimes a weak key may bring some hidden dangers to users, but before a security incident actually occurs, in the eyes of most users, a password like "123456" still protects their account security, and they also firmly believe that their account is safe. But if you force them to set a password that can't include birthdays and names, and has to meet a lot of extra conditions, it's entirely possible that they won't remember the password and need to reset it every time. In the end, their password became their recovery email instead because essentially it was always that email that allowed them to successfully log into their account and receive the reset password email. While the attacker cannot log into their account directly through the password, the attacker can choose to log into their recovery email and use the password reset link to log in to the account. Since the users themselves cannot remember the password for a long time, they cannot judge whether their real password is wrong, or the password has been maliciously tampered with by others. Especially when they do not use a real-time email client, if the attacker clears all the emails generated when changing the password, they will not be able to learn from the email that the password has been maliciously tampered with by others. At this time, the strong password policy has played a completely negative role. However, if you use a password policy with low strength requirements to ensure that most users can set a password that they must remember, users will realize that their accounts may be compromised by others when they cannot log in with their usual passwords and their accounts are invaded. Here is a practical suggestion for platforms that serve the elderly. Since most elderly people have poor memory, more consideration should be given to how to prevent them from memorizing passwords when designing the system. For example, the vast majority of elderly people now have mobile phones, and it is entirely possible to require an input of an SMS or other 2-step verification code every time they log in instead of entering a password. That way, they don't have to memorize passwords, nor do they have a password that an attacker can brute force. Or, if they do have a simple password, at least they can remember it and are still protected by another factor.

B. *Why Not Just Take It Easy?*

Some users are always worried about their privacy being leaked, so they strictly control all options related to permissions. But in fact, here is a different point of view that is worth everyone's reference. Although this point of view does not come from the field of information security, it comes from a saying in Jian's hometown of Beijing: "People have to live transparently." One level of meaning is to hold fewer secrets and be more open to others. Although it is impossible for a person to not have a secret, a person without a secret simply has no leverage for an attacker to snoop on. If users can summarize their personal information and clarify which information must not be disclosed, which information will not have any impact if others know it, and which information can be completely disclosed, then privacy protection strategies will be easier to formulate. If more information does not have to worry about being published, then the work of privacy protection will be easier. Like Jian himself, he never sets Instagram posts to be visible only to friends. People can indeed easily obtain his identity and some resumes, which in turn leads to the fact that no one needs to dig into his privacy to know his personal information. Instead, some of his more important private information is protected, because people who dig up his personal information just out of curiosity no longer need to collect a lot of information to understand him at this time. Of course, he also dared to disclose personal information because he has some anti-fraud capabilities.

V.DEFENSE

Social Engineering and the general public's unawareness of the sensitivity of personal information combine to make an incredibly potent weapon. Considering this, how do companies with large teams of internet-connected workers protect themselves from the threat of hackers exploiting this massive attack surface? One approach might be to tighten down company computers as much as possible, and effectively limit employee freedom. Another common approach is security training. Many companies recognize that security training is critical, and rightly so. In ProofPoint's 2021 "State of the Phish", they report that 57% of respondents surveyed experienced some kind of successful phishing attack. A full 74% of U.S. organizations were victims of a successful phishing attack at that time. Furthermore, 60% of successful phishing attacks resulted in a loss of data. Clearly, phishing is a data privacy disaster, and many companies are starting to recognize this. How bad varies significantly based on location, but phishing is a major issue regardless of location.

Security training can seem to some companies like an overly expensive or intimidating practice to implement when nothing has gone wrong. Whether it is worth the effort depends on the risks, the costs, and how much it can benefit a company. So, what does it take to make an effective security training program, and will it be worth the investment?

Unfortunately, it can be difficult to find concrete information on the effectiveness of social engineering training used in practice, and there are many interconnected variables that may impact its effectiveness, making this a difficult topic to study. Firms providing training do not want to give away all their information, but many publish either anecdotal or concrete information in some way. Hadnagy and Fincher run such a firm and have written extensively about what techniques tend to lead to successful security training campaigns. The most important thing is to keep training frequent, so it is always at the back of an employee's mind, but to not overwhelm them with attacks that are too difficult. If a company begins testing its employees with the most difficult phish, they can, will feel dejected, and like they will never be able to detect phish, losing all motivation. Proofpoint emphasizes the same ideas, suggesting phishing tests every 4 to 6 weeks (about 1 to 1 and a half months). Proofpoint also emphasizes the importance of making sure employees do not feel incapable, for instance by avoiding the use of jargon. They also point out that "jargon" may be broader than a security trainer realizes. A full 67% of people surveyed in the State of the Phish 2021 were either wrong or unsure of the definition of "ransomware", for instance. In general, it is important to note that an average employee is much, much less aware of computer security than the people training them. Another surprising statistic to this effect, over one-third of Proofpoint's U.S. respondents automatically trust an email with a familiar logo. Beyond just phishing tests, it is important to conduct company-wide security training.

Phishing tests may help detect how your company is doing, but for employees to know what they are doing wrong, explicit training is an important step of the process. For example, phishing tests won't detect a post-it note on an employee's computer. Furthermore, these training are often hyper-focused on one or two topics (particularly on email phishing), but there are many vulnerabilities that can affect a company due to employee error that many employees are totally unaware of (Vishing, strong passwords, insider threats). Once employees have been trained, they only need to be reminded in small chunks for their training to remain effective. Reinheimer et al. found that reminding employees 6 months after security training made a measurable impact on their ability to detect phish compared to employees that received no such reminder. An interactive lesson was slightly more effective than a video, which was more effective than text, which was much more effective than a short text reminder. All reminders other than short texts lasted 8 minutes. Employees who got an 8-minute reminder were nearly as good at detecting phish as they were immediately after a multi-hour training session, and far above baseline levels, showing that consistent training is highly effective at improving phish resilience. And, training does not need to take a large amount of time or resources as long as employees have already been made familiar with security concepts beforehand. Employees should also be made aware that their security is not important for only the company - if they are the victim of a successful phish they could have data stolen or suffer great financial losses.

One way to improve resiliency against phishing beyond training is to make it easy for employees to report phishing. Some security agencies will offer a convenient button in an email client (for instance, Proofpoint offers "PhishAlarm," and KnowBe4 offers the "Phish Alert Button"), which can help improve phishing detection and also makes security more convenient and ingrained in the company culture. Proofpoint found that with their system, some customers can get employees to report spam up to 60x as frequently as falling for it. However, this is an exceptional case, and the average value is only 1.2x as many reports as failures. Just having a convenient way to report does not mean employees will be aware of phishing or will use it. However, it can certainly help detect if a phishing campaign is occurring.

The main takeaway from considering reports of security training agencies is that security testing needs to be frequent, and constant - not a response to a security incident. And, employees should not be made to feel ashamed about falling for a test phish. They should be able to see themselves and their peers succeed sometimes, and then the difficulty of training can be increased until employees are phishing experts. One more important point made by many agencies is that training should mimic real phishing as much as possible (without being hurtful). If a real phish pretends to be from Microsoft, training should mirror that. If real phishing arrives every day of the week (it does), training should mirror that.

Notably, the vast majority of companies perform at least some sort of security training, including 100% of companies surveyed by ProofPoint in the US and UK. However, many companies do this in a more limited capacity than is necessary to see true returns. Of course, data reported by firms hoping you will purchase their products should be taken with caution, but the prevalence and success of phishing show that companies still have a lot of work to do, and the advice presented here is a good starting point. It is also notable that the United States often performs quite poorly when it comes to phishing awareness/resilience, and allocating more resources to training may help this.

VI.Conclusion

Although personal privacy is always leaked inadvertently and continuously, and we cannot completely prevent privacy from being leaked, the countermeasures a person takes determine whether it will develop into a disaster or appear to be nothing. We should always pay attention to the topic of privacy leakage, even if it can never be solved, there will never be a standard and universal answer. But our attention can always bring new ways to deal with it for more people. Although some of these new methods may be wrong, we always need more people to practice before they can be verified. Only when more methods are contributed, can better methods be continuously obtained in the changing social and network environment.

Acknowledgments

This paper is the final paper of the course Data Privacy. The content of the course was guided by Professor Zeyu Ding. Most of the content of the paper was inspired by the social engineering series, and all content was independently written by Jian and Ethan without any financial support.

Reference

[1] Lab, Kaspersky. "What Is Social Engineering?" usa.kaspersky.com. AO Kaspersky Lab, September 8, 2022. https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

[2] Klimburg-Witjes, Nina, and Alexander Wentland. "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses." Science, Technology, &amp; Human Values 46, no. 6 (2021): 1316–39. https://doi.org/10.1177/0162243921992844.

[3] Hadnagy, Christopher, and Steve Wozniak. Social Engineering the Science of Human Hacking. Newark, NJ: John Wiley &amp; Sons, Incorporated, 2018.

[4] Dreeke, Robin, Michele Fincher, and Christopher Hadnagy. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Newark, NJ: John Wiley &amp; Sons, 2015.

[5] Cosgrove, Adenike. "Employee Cyber Awareness Crisis". Infosecurity. Accessed December 7, 2022. https://www.infosecurity-magazine.com/blogs/employee-cyber-awareness-crisis/

[6] Baezner, Marie; Robin, Patrice. "CSS Cyber Defense Hotspot Analysis: Stuxnet" CSS Cyberdefense Hotspot Analyses. 2017. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/200661/1/Cyber-Reports-2017-04.pdf

[7] Fondrie-Teitler et al. "Tax Filing Websites Have Been Sending User's Financial Information To Facebook". The Verge. November 2022. https://www.theverge.com/2022/11/22/23471842/facebook-hr-block-taxact-taxslayer-info-sharing

[8] Heiligenstein, Michael X. "Facebook Data Breaches: Full Timeline Through 2022". Firewall Times. January 2022. https://firewalltimes.com/facebook-data-breach-timeline/

[9] Jordan, Daly. "Does Security Awareness Training Work" Usecure. https://blog.usecure.io/does-security-awareness-training-workProofpoint. "State of the Phish 2021". Proofpoint. 2021. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf

[10] Lee Moran. "Illinois Woman Arrested After Posting Selfie Wearing Dress She'd Stolen," July 21, 2014, https://www.nydailynews.com/news/crime/woman-arrested-selfie-wearing-stolen-dress-article-1.1874408

[11] Markowitz, Erik. "16-Year-Old Live-Tweeted Bomb Threats for 3 Months Before he was Arrested" Vocativ. https://www.vocativ.com/underworld/crime/16-year-old-live-tweeted-bomb-threats-3-months-got-arrested/

[12] Reinheimer et Al. "A An investigation of phishing awareness and education over time: when and how to best remind users" Usenix 2020. https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf

[13] Surette, Ray. "How social media is changing the way people commit crimes and police fight them" University of Central Florida. 2015. http://eprints.lse.ac.uk/65465/1/blogs.lse.ac.uk-How%20social%20media%20is%20changing%20the%20way%20people%20commit%20crimes%20and%20police%20fight%20them.pdf

[14] Tischer, Matthew at al. "Users Really Do Plug in USB Drives They Find" 2016 IEEE Symposium on Security and Privacy. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7546509

[15] US Department of Justice. "Criminal Use of Social Media" US Department of Justice. 2011. https://www.ojp.gov/ncjrs/virtual-library/abstracts/criminal-use-social-media

[16] Verizon. "2019 Data Breach Investigations Report" Verizon. 2019. https://www.verizon.com/business/resources/reports/2019-data-breach-investigations-report.pdf

[17] Zetter, Kim. "LifeLock CEO's Identity Stolen 13 Times" Wired. May 2010 https://www.wired.com/2010/05/lifelock-identity-theft/