Behind Every Great Computer There Is a User

Matthew Gaudrault

Charleston Southern University

Principles of Cybersecurity CSCI 405

Patrick Hill

3/13/2024

Abstract

As computer systems become increasingly advanced, so too must the users increase their knowledge on how to protect their data and their systems. In this paper we look at 3 ways that bad actors exploit users to make money. By selling their data, ransoming data, and tricking the users into thinking the bad actors are someone other than who they are. We look at how much money can be made from selling data and what type of data is typically targeted. We then look at how some ransomware works both for personal computers and in the company environment. Then we discuss ways that bad actors trick users into thinking they are family or friends and need financial help. The paper concludes with ways that we can help protect they data and what we can do as users to stay ahead of the bad actors.

Problem Between Keyboard and Chair

The typical IT Help desk trope of stating that the user is the problem can be seen as highly accurate for most cases depending on who you ask. As you think about this from a Cybersecurity point of view, it can be argued that it is still true. When I first went to college straight out of high school, my school email was very bland. Mainly just updates on upcoming events or upcoming due assignments. Now your school email gets phishing attempts year-round. Since coming to CSU, I feel they have averaged about once a month or so and are typically followed up shortly with an email from the security team stating not to trust or use the link. I have not clicked on them so I could not tell you if some of them were from the security teams themselves as a learning device for younger classmen that might not have as much experience with those sorts of interactions. Some of them do seem pretty tempting and when I was a freshman, I would have probably clicked on one or two because let's face it, how many lower classmen wouldn't love an extra $500 for helping with something? Money is tight as a student, and you can only ask your parents for money so many times before being scolded. The reason you see more and more of these phishing techniques are because of how effective they are. As computers ever grow more powerful, people have to learn to adapt to stay ahead of the bad actors associated with manipulating people and security systems to earn their money through selling data, ransoming your data, or even tricking you to pay by making you believe you are someone else.

Selling data can be very lucrative for bad actors. According to a 2017 study, the cost of cyber attacks could be as high as $400 billion (Shachar, 2017). This comes from many different angles but one such way is through selling data. There are multiple avenues in which to sell the data depending on what type of data has been stolen. Personal Identifiable information (PII) is the most sold data and has many uses. PII has many uses from things as simple as helping your shopping browsing to more devious like stealing your identity. Many applications that you download on your phone allow access to your PII.

One major step that can be taken to help limit what data you share and who you share it to, is by reading your terms and conditions when signing up for things. Many times, these are very lengthy and listed in a way to make it difficult to understand them all. This is why many users just hit accept and do not read through what is being shared. Companies have used the data collected to sell to other companies who would be interested in it for targeting individuals for many reasons from shopping to exploiting individuals specifically. If the right person is found this PII data can be used to fish for other types of information from that user. For example, if a person's data is found to see they have a lot of debt and are working for a certain company, then bad actors could try to use that to have the user steal intellectual property data from their company. The data they have on the user could also lead to them ransoming the user to feed the bad actors the data they want from the company itself.

Sometimes the bad actors do not want to deal with the middleman (the user) and will go directly to ransoming you or your companies' data directly. I have personally encountered this with many viruses. When I started my IT career, I was in a smaller IT help and repair center outside Kiawah and Seabrook Island. Kiawah and Seabrook are both higher scale communities with most of their populations older than retirement age. This set them up as being targeted often by viruses and other schemes. I saw a wide range of viruses from redirect viruses, to pop-up adds, to spyware acting as virus-removal software, to ransomware. The ransomware would take over the entire computer and present a message stating you needed to pay the company to have access to your data/computer. This first one I encountered was one that took over the screen and stated that it was the FBI and the user would need to pay a certain balance to prove that they are the correct user. Although it was made to look like a true FBI site, it was just ransomware and we at the computer store had to remove it to restore function to the computer. Many times, the user had already paid and their computer was still not unlocked, this is where we tried to train all of our customers to reach out to us first and not give into the ransomware. The ransomware can accidentally be downloaded from a mis click while browsing online or from

downloading the virus from an email attachment. Even if the data was relatively protected by not having direct access to those outside of the home or computer user, the bad actors knew how to target the weak link of the users themselves. This same process can be used on company data as well. "In 2022, one cyberattack led to stolen customer data, which was held at ransom for $9.7 million. Before legal fees and customer compensation, this security breach cost the organization between $25 and $35 million" (Reid 2023). Attacks like that one not only have a monetary cost but also hurt the reputation of the company that lost the data. This can be seen through attacks like the one suffered by Monster.com. Since they were repeatedly found to have lost data the financial hurt of the attack itself would be considered small compared to the damage their company image suffered.

The 3rd way scammers or bad actors can cause users to suffer is by extorting money out of the user by making them believe the actors are someone else like a family member or a friend of the user. I have witnessed this style attack twice in person, at the same IT help company mentioned above and then again with my own grandmother as she was scammed out of $16000. At the store we had someone come in stating that her email was acting weird and that a friend had called her about a suspicious email. After looking at her computer, we discovered that her email account reply address had been changed to an alternative email and so she did not receive any of the responses. The bad actor had sent out an email to many in her address book stating along the lines that she was stranded on vacation and was asking her friends and family to wire her some money. This is a scammer preying on the kindness of friends and family to help and hopefully not as many questions. It is a pretty straightforward scam as it was just send out an email and redirect the reply to a box that they monitored, most people would not even realize the change. As computers become more cutting edge so have some scamming techniques. This is what my grandmother experienced, it was not from an email, but she received a phone call from who she thought was my brother, her grandson. The police were contacted days later after she figured out it was a scam but swore that it was my brother's voice

she heard on the phone. The detective who was looking into the scam told her that it is becoming more and more common for scammers to use people's online presence to mirror or fake a family member or friend. The scammer was very talented as he knew what to say and do to get money out of my Grandma, and even guided her on how to withdraw the money out of the bank without setting off flags. With the increase in AI and the increase of data that is being posted online with facebook, Instagram, and tiktok, I'm sure attacks like this will increase in popularity. Trusting elderly family members can be easy targets, especially if they love to talk on the phone as much as my Grandma. Looking back, she felt silly for falling for a call needing money to cover a car accident/medical bill but at the time of the call she just wanted to help my brother in a tough situation.

Conclusion

So, whether the money is coming from selling data, ransoming the data, or from asking for money directly from the person who is being scammed, the common denominator is the user. Some tips from Forbes magazine for better protecting data are the following 3 steps: "Be skeptical of unsolicited messages, Keep your software up to date, and Use strong passwords and two-factor authentication" (Dinha, 2023). These are great steps to get started with protecting your data as being skeptical of messages can help you avoid phishing attempts as well as help you from accidentally downloading malware. Keeping your software up to date will also help with malware as the software is constantly fixing any exploits that are found with malware. Dual-factor authentication helps eliminate a user's password as being the weakness. It is cumbersome to remember all the different passwords for multiple logins, so many people will repeat the same passwords over many accounts. This means if one account login is found then that information can be used to gain access to many other accounts. Dual-factor authentication can help eliminate that as you would need more than just a password. According to the security week article, "It isn't all about employees maliciously ignoring the rules." (Prince, 2015). This article points out the fact that there must be a good balance between the user and the compliance

built in to help protect the business. A lot of the help needed comes back to training and continuous training because the world of cybersecurity is always changing and evolving.

Another point of emphasis from the security magazine is that we must change the way that the users think. The article does a great job of comparing IT security to something that a lot of us deal with in a more tangible way, locking your vehicle. Tourinsky writes, “If the door is locked, they move on. If it’s unlocked, they grab whatever is easy – spare change left in the console, sunglasses left on the seat, a laptop left in the trunk. The solution is pretty simple—lock your car doors to reduce your chance of something getting stolen.” (Tourinsky, 2021). This helps people who are not computer minded visualize cybersecurity in a more understandable way as many people have either dealt with a car break-in or know of some who has. If the user makes it easy, then they will be more likely to be broken into or have their data taken. If the car stays locked then the driver cannot get in, so that is why it is the driver's responsibility to lock the car when not in use. Just like how it is the user’s responsibility to protect their data and their system by being mindful of the environment they are in.

References

Dinha, F. (2023, April 11). *Council post: The human factor in cybersecurity: Understanding Social Engineering*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/04/10/the-human-factor-in-cybersecurity-understanding-social-engineering/?sh=12fe5a1c6a02

Prince, B. (2015, January 15). *Employees not following policy is the biggest threat to endpoint security, it Pros say*. SecurityWeek. https://www.securityweek.com/employees-not-following-policy-biggest-threat-endpoint-security-it-pros-say/

Reid, J., Atterholt, J., & Cellini, A. (2023, September 8). *The human factor in cybersecurity: Crowe LLP*. Crowe. https://www.crowe.com/insights/the-human-factor-in-cybersecurity

Shachar, A. (2017, June 22). *Cybersecurity – the human factor*. Federal information System Security Educators Association. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

Tuorinsky, E. (2021, September 2). *The human factor in cybersecurity*. Security Magazine RSS. https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity