Global Knowledge®

Expert Reference Series of White Papers

Human Vulnerabilities in Our Current Threat Landscape

Human Vulnerabilities in Our Current Threat Landscape

The Hacker Academy, a Division of Blackfin Security Group

Introduction

Forty-three percent of companies experienced a data breach in the past year. This number is staggering, especially when you consider the amount of organizations that could have been breached without even knowing or without properly reporting it. It's impossible to defend against every threat out there, but what is possible is setting up the best defense mechanisms you can to decrease your chances exponentially. This means more than just setting up a bunch of hardware with blinking lights and sirens. It means taking a proactive approach to securing your organization's front line—the humans.

When looking at today's threat landscape, humans are proving to be one of the most vulnerable links in the information security chain. The problem with this is that so many times it is a human decision, not a technological one, which allows the threat to come to fruition. If one chooses not to take secure measures, the vulnerability is human, not technological.

From sending sensitive information over public wireless connections to clicking on malicious links in phishing emails, expensive mistakes are being made every day. There is no end-all solution that will thwart all of these attacks, but there are controls, such as taking steps to educate users, which can be put in place to increase resiliency.

The purpose of this paper is to help organizations of all sizes understand the current threat landscape as it pertains to human vulnerabilities, and how to take the first steps toward mitigating them. By the conclusion of this paper, you should be able to:

- Understand what attack vectors are being used in attempts to breach your network or steal information
- Recognize what employee behaviors may be putting your organization at risk
- Develop a strategy to better inform your users of these threats

Understanding Threats and Attack Vectors

An attack vector is the approach used to assault a computer system or network. A fancy way of saying "method or type of attack," the term may refer to a variety of vulnerabilities. There are countless ways in which an employee's weaknesses can be exploited by attackers. Understanding where the vulnerabilities and dangers lie is the first step in creating a successful mitigation strategy. The following areas are pain points experienced by organizations across all industries.

Phishing

By definition, phishing is the practice of using fraudulent emails and copies of legitimate websites to extract private information and data from computer users for illegal or malicious reasons. We've all gotten them before, but have we been able to identify these scams? Every email user at some point in time will get some sort of phishing email, it's nearly guaranteed, and our chances are rising each day.

So, what is the end goal of attackers who are carrying out phishing attacks? People phish in order to either obtain information or to drop malware that can be deployed instantly or at a later time. That "or later" part is very important because you may not always see the consequences or effects immediately, it may take a good while. At the end of the day, we're dealing with social engineering through electronic delivery. The more creative our electronics capabilities get, the more opportunities bad people will take to exploit those new technologies.

There are a few different types of phishing attacks everyone should be aware of:

- **Smishing**: Phishing using SMS Texting, prompting an action such as a phone call or clicking on a link.
- **Spearphishing**: Much more targeted attacks that usually pertain to a very small group after some amount of research on the targets has been conducted.
- **Whaling**: Phishing attacks that are specifically going after executives. A lot of the time on a one-by-one basis with information acquired through research or from previous successful spearphishing campaigns on colleagues.

The most unfortunate part about these types of scams working is that they are typically easy to avoid. But what happens when it's not so easy to identify them? With the onslaught of private information becoming public facing through social media and social networking sites, phishing attacks are evolving. They are moving away from the original emails we would see, which were littered with grammatical errors and spelling mistakes, and are starting to mimic, or spoof, legitimate correspondence that may come from our colleagues, banks, schools, or even families.

There are two main ways in which we can empower our users to better recognize and report phishing attacks:

1. **Training:** Inform your staff of certain triggers and cues they can look for that will enable them to become another sensor sitting on your network. Let them know what to look for in emails that appear "phishy" and give them a clear line of communication to a security expert who can help them determine whether it's a legitimate email.
2. **Assessments:** The training portion is good. You've got an awareness program set up, and your company has taken a great first step. But, how do you actually test whether training is working? You're going to perform assessments. This is your way to test practical knowledge. You will mimic attack-type behavior to familiarize end users with tactics that are being used today. Between this and your training, you're going to teach users to recognize difference cues and trigger through mock-phishing email campaigns.

Appropriate Use of Email and Instant Messenger

In our modern world, email and instant messaging platforms have allowed for a greater ease of near instant communication globally than ever before. Like all communication, regardless of form, it only remains beneficial through the ways we apply it. Online interactions need to be thought of in the same ways we treat our real-world interactions. The most important thing to first keep in mind about online interactions is that what you write and publish is permanent. It is no different than writing something down in ink in the real world. As soon as you save or send an email, or send an IM, it is also permanent. It exists in most cases, forever, even if you delete it. It is stored on a server, somewhere in the world.

Keeping in mind that permanency; never at any time should Internet users send private information via email or IM. It may seem like email is completely secure and that nobody can break into personal or work email accounts, but it happens every single day. Things like user names and passwords, credit card numbers, bank account information, and social security numbers—none of them should be sent via email. These sorts of information are best left to a quick thirty-second phone call. Having that kind of information sitting in someone's email account is a recipe for disaster. All it takes is that inbox to be compromised by a hacker for everything to be taken.

As a general rule, just as in real life, if you'd second-guess revealing information in public while in person, or if you wouldn't want everyone to know a certain piece of information, then it has no place in an email, on IM, or the Internet in general. It's better if said in person.

So what should be transmitted via email then? There are some basic principles that should be kept in mind prior to sending anything:

- Threats, harassment, and inappropriate conversation have no place in email or IM. It is also a good standard to avoid controversial conversation topics such as politics, sexuality, and religion—you can never been too sure when such conversations will offend, or be taken as harassment. In the case someone respectfully asks that you stop a certain path of discussion, or feels a conversation is inappropriate—you are to stop all messages immediately.
- A mass email is a message you and a long list of people have received at the same time, from a mutual friend. They're usually shared emails containing jokes, stories, or other sometimes useful information. They can be enjoyable, but only when we put the proper forethought to if and how we share them. Mass emails go out to a lot of people, most of whom may not know they're about to get a mass email. They can be further inconveniencing to recipients because they can interrupt and bother people during busy workdays. The other point to mass email forethought is the address field used. When you send an email, and you include a number of email addresses in the "To:" field, all the people receiving that email can see each other's' email addresses. For some, that's incredibly invasive and a violation of their privacy. It's the same as someone giving your address or phone number to someone you don't know. To be considerate, and safe, for all parties, the "BCC:", or blind carbon copy, field should be used. It hides all other addresses except the receiving party's from each other.
- Interactions on the Internet should be treated like private conversations between friends. If you don't think you're supposed to repeat the information you read in an email, much like you wouldn't tell a friend's secrets and personal information, then you should never forward it.

Working Remotely

We live in a very different world than we did fifteen, or even ten, years ago. It was only a few years ago when the only places that you really got to do focused work on a screen were in your home, at school, or at work itself. But the world has changed and we blame coffee shops. Starbucks made it their mission to create a "third place" that was neither home nor work, but gave you the comforts and the ability to do all the things you'd do in either of those. And now, that third place is everywhere. You are probably able to do work as effectively from home, at a coffee shop, in an airport, even in an airplane at 35,000 feet as you do while you're in the office.

But just because we may not be at the office doesn't mean your work security concerns change. All of the same PII, Privacy, Data Protection, etc., issues still exist, and in fact, some of them become more important to think about when working remotely.

Imagine you're in a local café working remotely. While you're sitting in the shop, enjoying a cup of coffee or tea, you're steadily working on some reports that are due in a few days. While concentrating and working away, you even begin to lose notice of the rest of the coffee shop around you. That type of concentration isn't a problem when you're in your regular office place, however, as you're surrounded by trusted fellow employees. Unfortunately for us, these "third places" are very good at getting us to let our guard down.

These are all examples of considerations that need to be addressed when working remotely.

- In your concentration, do you notice where you're sitting in relation to everyone else?
- Can someone read your work data over your shoulder?
- Is someone reading over your shoulder?
- Did you leave your laptop at your table while you went to the washroom?

The solutions to the additional problems are easy:

- When working in a public place sit at a seat where your back is against the wall of the establishment. It makes it impossible for someone to read over your shoulder from behind you. Simple as that.
- Never leave any of your devices alone. Laptops, phones, and tablets today are light and portable. This means that they're easy to carry with you as you get up from your seat. This also makes them incredibly easy for thieves to steal. Whether you're getting another cup of coffee, or going to the washroom, if you leave your seat then the devices should leave with you. This completely eliminates any chance someone can look through, or even steal, your devices while you are away.
- Keep all of your security controls up-to-date, and in place. This is something you sometimes don't have to worry about when at the office. Most of these things are controlled by your security team. But just because you're not at the office doesn't mean security is any different than when you are. Rather, it's more likely the case that there is a greater importance placed on maintaining and monitoring the security measures that exist on your work devices. This means making sure any security software is in place and up to date. Make sure you're using secured browsing, and that your browsers and operating systems are up to date.
- Begin to really think about what type of work you're doing when in public spaces. Even with security controls in place, it can be easy for an attacker to hijack your network connection while at a café.

All it takes is a few moments of thought about our actions as we apply the responsibility of working remotely.

Social Engineering

Everyone should be very familiar with the idea of social engineers. These are people who make their living taking advantage of others. Social engineering works because we as humans are wired to help people. It may be good will, or it may be social pressure, but there is no doubt that it exists. If someone comes up to us and asks us to watch their cart in the grocery store, chances are, we do it. If someone asks us for directions, we tend to want to help them. If someone asks us to hold that door because they're carrying a heavy box, we help make their day a little better; it's in our nature. But what about when holding that door meant they just walked in to a secure area? "Tailgating" is an incredibly popular social engineering technique, because it works so often.

What makes social engineers effective in the real world is that they are aware of that hard-wired behavior, and they have learned to take advantage of that. They can take our human nature and turn it against us, and those tricks often work when trying to socially engineer a business. Think about your office. How often do you see the food delivery guy; someone delivering a sandwich, or a pizza? When was the last time you checked to see if that delivery guy was actually delivering food? Sometimes the most simple social engineering tricks work the best. Something as simple as a blue polo with a black baseball cap and a $10 pizza can give a social engineer almost unlimited access to an office. Then, all they have to do is slip a thumb drive into the back of a computer as they walk around, "looking" for who they were supposed to deliver the pizza to.

These attacks can also happen over the phone, too. Jim from IT is on the phone, and he wants your log-in information. There are a few things which need to be considered in a situation like this:

- Is there even a Jim in IT?
- Why would IT be calling for your log-in information?

Start asking these types of questions when sensitive information is being asked for over the phone. And these phone attacks are especially dangerous, as you do not get the luxury of seeing who you're speaking to. Stopping these sorts of attacks at the office is simple if the habit of questioning people is developed. If you see someone walking around without an escort, ask them who they are there to see, and when they answer, take them to that person. Or if they can't answer, go ahead and escort them back to the security desk. Unsure of someone on the phone? Ask to call them back, so you can verify who they are. Shutting down a physical social engineering attack is as simple as that.

Mitigating Human Vulnerabilities

Now that we've identified and discussed just a few of the human vulnerabilities that exisit, the question then becomes, "How can we, as security professionals, protect our colleagues, thus protecting our network and inform our staff of the above risks?"

It starts with education.

As technology is racing ahead and we are desperately trying to catch up, it's becoming clear that few people have the understanding to implement the necessary cybersecurity measures required for an organization. People cannot change and become better sensors unless they are aware of how they should be behaving and what they should be looking out for on a day-to-day basis.

The first step to creating a more "aware" culture in your company is by implementing a cybersecurity awareness program. If you choose not to implement effective and efficient security policies, the vulnerability is strictly human, and cannot be blamed on technology. So, where do you start?

There are three main roles your awareness training should play.

1. **Legal or Regulatory Compliance:** In some cases organizations are forced to comply with regulations such as HIPAA or PCI. These regulations are most commonly put in place in organizations that handle extremely sensitive information such as personal health or payment card data.
2. **Security Literacy:** It is necessary to create a common language on which to build other efforts. This will, in turn, create a common base of knowledge and vocabulary on which to build behavioral competency. It does not, however, create that behavioral competency.
3. **Behavior Design:** Behavior design often includes three different factors. The likelihood of getting actual behavior change increases when all three are present.
    a. Sufficient **motivation** to perform the behavior
    b. Sufficient **ability** to perform the behavior
    c. We get **triggered** to perform the behavior at the time when motivation and ability are present

The combination of a strong policy combined with cyber security awareness training is an approach that embraces the human factor as an asset instead of a detriment. This approach, compared to the alternatives that focus solely on software and hardware, modifies behavior and builds a culture that is aware of the threat landscape and how it affects them directly. It encourages the conversations between your security teams and end users to take place, and fosters the beginning of what could be a multi-million dollar savings approach to recognizing and mitigating the human vulnerability.

Conclusion

Times are changing. Attacks are becoming much more sophisticated and hackers are exploiting human vulnerabilities to gain access to enterprise networks and private information. It's unrealistic to expect a 100 percent impenetrable network, no matter how much time and money are invested in security products and training.

Employees and end users want to help protect your company's sensitive data, we just need to motivate them as to why they should care. By educating your employees on security best practices and current human vulnerabilities, you can take a step forward to ensuring you're not a part of that 43 percent of organizations that were breached.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- The Hacker Academy Training Bundle (12-month subscription)
- Cybersecurity Foundations
- Fundamentals of Information Systems Security
- Social Media Security Professional (SMSP) Prep Course

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.