November 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people

Identifying the Pretext

Pretexting Explained

Pretexting Techniques

How to Spot Scams

PRETEXTING EXPLAINED

Behind almost every successful scam is a well-crafted scenario. Scammers harness the power of good storytelling. They know that if they can create realistic, believable scenarios, they increase their chances of tricking someone into divulging information or sending money.

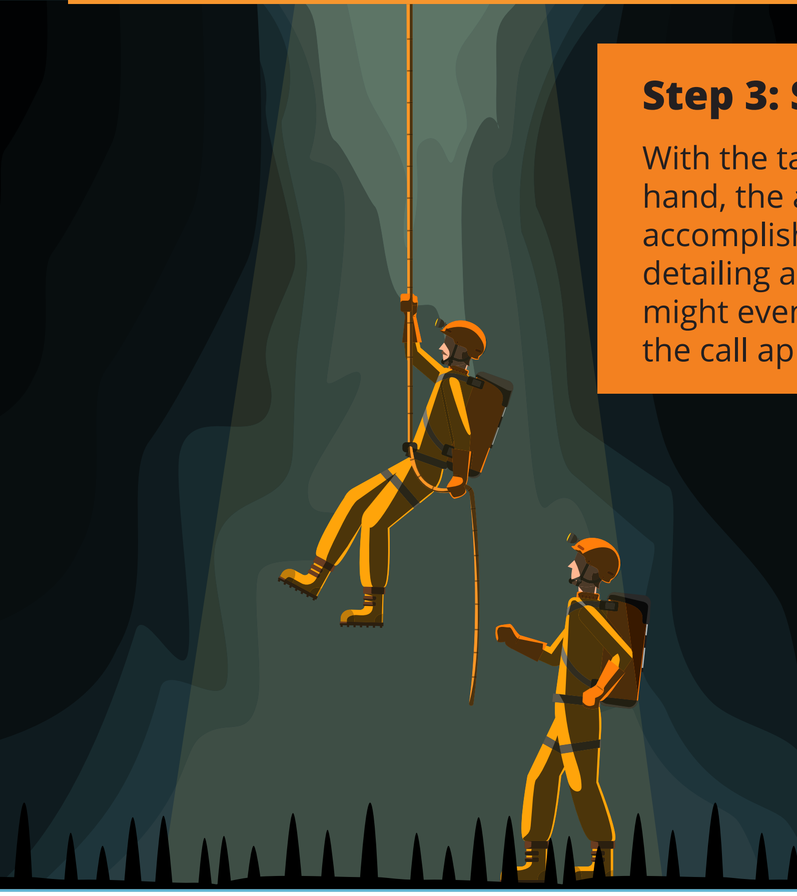
It's a process known as pretexting—the art of manipulating people with falsified stories. Pretexting thrives on gaining and abusing trust. Here's an example attack broken down step-by-step from the scammer's perspective.

Step 1: Identify the Target

Research leads to successful attacks. Scammers will do their best to gain information about specific individuals or job roles. They use public forums like social media to research people and collect information, which can ensure a smooth transition to the next step.

Step 2: Develop Credibility

For a scam to work, the attacker must present themselves as someone credible and trustworthy. This usually involves the impersonation of someone the victim knows. Common examples include impersonating executives, customer service agents, and even family members or friends.



Step 3: Set Up the Scenario

With the target identified, and information about them in hand, the attacker will attempt to gain trust. This is typically accomplished by calling the target on the phone and detailing a plausible scenario. In some cases, the attacker might even use tools that can trick the caller ID and make the call appear to come from a legitimate business.

Step 4: Vanish

Whether the goal was to gain access to confidential information or defraud the victim of money, the attacker will quickly vanish once successful. Hopefully, the attack will fail, and hopefully, the target will report the incident immediately so the organization can warn others of potential scams.

PRETEXTING TECHNIQUES

Pretexting utilizes old-school techniques with a few goals in mind: steal confidential information, gain unauthorized access, or defraud people out of money. How do scammers achieve those goals? Most of the time, they just pretend to be someone else. Let's explore four common scenarios.

The Bank Representative

One of the most traditional scams involves a phone call from someone claiming they work for a bank where you have an account. They calmly tell you that they've noticed some unusual activity and had no choice but to freeze your funds. To unlock them, they simply need you to confirm your username and password.

The Friend Who Needs Help

If someone falls victim to a phishing attack, they could lose control of their social media profile. The attacker can then use that profile to send messages like this: "Help! I'm traveling internationally and lost all of my bank cards. Can you wire me some money so I can buy a ticket home?"

The Manager

If your boss or manager emailed you asking for highly confidential information, what would you do? A lot of people tend to quickly respond to requests that come from authority figures. That's why scammers attempt to impersonate executives and others in management positions.

The Tech Support Agent

Are you having computer problems? The scammer posing as a tech support agent sure thinks so and hopes you'll believe it. This common scheme attempts to defraud people out of money by convincing them to pay for support services they don't need to fix problems that don't exist.

All four of these scenarios are based on real scams that continue to target organizations and individuals. You can avoid becoming a victim by remaining skeptical, verifying someone's identity before obliging any requests, and using common sense.

Here at work, be sure to follow policy, and report anything suspicious immediately!

HOW TO SPOT SCAMS

From phishing emails to suspicious phone calls, most scams can be identified by using a little common sense and staying alert for these red flags:

THREATENING OR URGENT LANGUAGE

Whether in an email, text message, or over the phone, threatening or urgent language is always a clear warning sign. Scammers want you to react before you have a chance to apply much thought to the situation. Any time someone asks you to perform an urgent action immediately, "or else," you can assume you're being targeted.

BAD GRAMMAR OR AWKWARD PHRASING

There are many ways to spot generic phishing messages. In particular, emails that contain poor grammar, incorrect spelling, or an awkward tone should trigger your skepticism. Be sure to hover over links to reveal their true URL before clicking. Unless you're absolutely certain an email is safe, don't click and don't respond. At work, report it immediately. At home, block the sender, and delete the email.

GIFT CARDS

Many cases of fraud involve asking the victim to purchase gift cards and reveal the payment details to the scammer. Since gift cards are essentially cash, they have no consumer protections built-in like credit and bank cards do. Remember that no legitimate organization or entity will ever ask you to pay for something with gift cards.

RANDOM TEXT MESSAGES

Phishing via text messages—known as smishing—has become more and more frequent over the years. A typical smishing attack features many of the same indicators we encounter with phishing attacks. Most notably, they'll fail to greet you by name or username, make a threat or an urgent call to action, and include a suspicious link. Always think before you click!

UNEXPECTED EMAIL ATTACHMENTS

Email attachments are one of the most common ways data-stealing malware infects devices. As a general rule, never open or download attachments that come from people you don't know. Even if you receive one from someone you're familiar with, don't assume it's safe. Carefully review the message and do everything possible to confirm its legitimacy before accessing the attachment.