UNIVERSITY SYSTEM OF GEORGIA
Cybersecurity

Supplement to Cybersecurity Awareness Training

Social Engineering

Why Do Attackers Use Social Engineering?

Quite simply, attackers use social engineering because it consistently works. There is no patch for a user who forgets, in the heat of the moment, to follow what they have been taught.

Social Engineering is the path of least resistance

Hackers know it may take hours, weeks, or even months to brute force their way into a network to steal credentials. On the other hand, social engineering tactics with the right ploy and a phone call or email the credentials can be stolen in just a matter of minutes. An attacker might try to gain physical access to a company's network computer, impersonate a delivery man, construction worker, or tech support. Sifting through open source information, dumpster diving, or talking with a disgruntled employee may yield information used to gain illegal access.

Once the attacker is inside the organization, a common USB thumb drive is all that's needed to infect a computer, gaining access to the network. Social engineering risks become greater as software products become more secure and harder to crack. Understanding the motivation and tactics of a social engineer enable us to identify an attack.

Typical Motivations

A malicious social engineer is motivated similarly to the average person in the work force. Knowledge is power, the more you know, the easier it may be to succeed. A malicious social engineer has some of the same goals that an average person may have but, with one difference—a lack of ethics.

Goals

Dr. Max Kilger identified six motivations for non-ethical computer activity. These motivations are money, cause, entertainment, knowledge ego and revenge. They exist in nearly any society. Each of these motivators can be considered a goal of social engineering. The ultimate goal is information which is needed to satisfy the motivators.

Listed below are primary motivations for social engineering attacks and links to copies of news articles where these motivations were used in an attack:

- **Money:** City of El Paso duped out of $3.3 million in phishing scam
- **Cause:** Hackers in Venezuela Hit Dozens of Government Websites
- **Entertainment:** Dark Overlord hacks schools across U.S., texts threats against kids to parents
- **Knowledge:** Nigerian Email Scammers Are More Effective Than Ever
- **Ego:** Three Hackers Plead Guilty to Creating IoT-based Mirai DDoS Botnet
- **Revenge:** Revenge Hacks Cost Former Employee 34 Months in Prison, $1.1 Million in Damages

Resist Phishing with These Three Golden Rules

City of El Paso duped out of $3.3 million in phishing scam

KVIA NEWS | Brenda De Anda-Swann | Nov 02, 2016 02:39 PM MDT | Updated: Nov 02, 2016 06:54 PM MDT

EL PASO, Texas - The City was "duped" and "robbed" of millions of dollars intended for the streetcar project, a source with knowledge of the investigation told ABC-7.

During a news conference Wednesday afternoon, city officials revealed a person or group pretending to be a vendor scammed the city out of about $3 million by using a phishing scam.

Phishing is when criminals pose as a legitimate person, business or agency to commit fraud. In this case, the fake vendor used email contracts to scam the city.

Dr. Mark Sutter, the city's chief financial officer, said the first payment to the phony vendor was for about $300,000 and a second payment was for about $2.9 million.

The fraud was detected by the city's Comptroller's Office, according to a city news release. In early October, the comptroller notified the internal auditor the city may had fallen for a phishing scam resulting in about $300,000 lost. Internal controls were placed and law enforcement was notified, according to the city.

A couple of weeks later, during the investigation, the city and the Camino Real Mobility Authority or CRRMA found "an additional misdirection of funds" of about $2.9 million, said the release.

Sutter said the city has recovered about half of that money: nearly $1.6 million from the $2.9 million, and $292,000 from the $300,000 payment.

El Paso Police and the FBI are working on the investigation.

"We were able to work with the banks and law enforcement and were able to get that money back," said Mayor Oscar Leeser.

Leeser, flanked by City Representatives Lily Limon, Cortney Niland, Carl Robinson, and Jim Tolbert, said little about the way the scam took place citing the pending investigation. He said giving more information could jeopardize the city's ability to recover the rest of the money. Leeser said they've reviewed all vendor payments and were able to ensure this was the only problem.

City Manager Tommy Gonzalez said "We want to reassure the public that this situation is under control."

City officials won't reveal how the scam happened, whether it was an oversight or a failure of the vetting system and whether anyone will be held accountable.

The city's news release states, "The City did not immediately inform the public about the phishing scam at the request of law enforcement to allow for an appropriate investigation and to increase the possibility of recovering the funds," however, City Attorney Sylvia Borunda Firth said during the news conference law enforcement didn't request that they not say anything, but advised them not to.

"More discretion will allow for a better investigation and more recovery of funds," she said.

"I know you have a lot of questions," said Leeser at the end of the brief news conference. "So do we."

Return to Motivations for Social Engineering

Hackers In Venezuela Hit Dozens Of Government Websites

NPR | Scott Newman | August 7, 20178:08 PM ET

Hackers in Venezuela attacked numerous government websites in protest of the "dictatorship" of President Nicolas Maduro.

A group calling itself "The Binary Guardians" said it hacked about 40 government sites, according to Reuters.

"Our intention is to give hope to people that no matter how strong the enemy seems, there is strength in unity," the group wrote in an email quoted by the news agency.

Reuters writes: "The country's CNE elections authority, which ran the July 31 vote for the new 545-member 'constituent assembly,' was among the sites hacked. Its hacked page featured a flyer in favor of Operation David, and a video showing a clip from Charlie Chaplin film *The Great Dictator."*

The hacker attack comes amid continued unrest and uncertainty in Venezuela a day after attack by armed men on an army base in Valencia.

NPR's Philip Reeves, reporting from Caracas, says Maduro's ruling socialist party is portraying Sunday's attack on the base as evidence of an attempted uprising against the government that is being instigated by Washington.

"His message was echoed by Venezuela's defense minister who, clad in combat clothes, made a passionate televised speech to hundreds of troops, who'd assembled for the cameras with their guns and tanks," Reeves says.

He says "thousands of government supporters were summoned to a rally in the capital Caracas [to support] Venezuela's new constituent assembly, a body many countries see as illegitimate — and a means of giving Maduro dictatorial powers."

Return to Motivations for Social Engineering

Dark Overlord hacks schools across U.S., texts threats against kids to parents

CSO Magazine| Ms. Smith | Oct 9, 2017 | 8:46 AM PT

Bad weather, natural disasters and the like can result in school closings, but some districts do shut school doors for other “credible” threats. Last year, creepy clowns caused panic and school lockdowns, but this year it is hackers threatening kids that has resulted in school closings across several states.

The hacking group responsible is the Dark Overlord, the group that leaked new *Orange Is the New Black* episodes because Netflix didn’t pay a ransom. The same group tried to sell millions of pilfered healthcare records and was responsible for other attacks such as on Gorilla Glue and an Indiana cancer service agency. Now, it is targeting schools and scaring the snot out of parents by sending personalized text messages threatening their kids.

[Read also: Hacker hijacks police radio broadcast until cops call off car chase of armed robbers and bookmark CSO's daily dashboard for the latest advisories and headlines.]

Iowa

On Oct. 2, the Dark Overlord hacked Johnston Community School District in Iowa and used the pilfered student data to send out threatening text messages to their parents. In response, the district district closed schools for one day and delayed classes by two hours on Oct. 4.

Some of the text messages were shared with the media. One read: “Your child is still so innocent. Don’t have anyone look outside.” When the parent told them to stop, the response was, “I’m only getting started.”

Another threat read, “I’m going to kill some kids at your son’s high school.”

Also on Oct. 4, the Dark Overlord publicly claimed responsibility, tweeting:

We're now publicly claiming responsibility for the threats that resulted in the closure of JCSD in Iowa and 7.200 children without school.

— thedarkoverlord (@tdo_hackers) October 4, 2017

The next day, the Dark Overlord dumped the stolen data on Pastebin. The now-deleted post included "student names, addresses and telephone numbers." The better to help child predators, they claimed.

With the student directory from JCSD we released, any child predator can now easily acquire new targets and even plan based on grade level.

— thedarkoverlord (@tdo_hackers) October 5, 2017

Why attack schools and threaten kids? "We're escalating the intensity of our strategy in response to the FBI's persistence in persuading clients away from us," a hacker from the group told The Daily Beast.

Iowa is just one in a worrisome string of school hacks that resulted in threats of violence to children attending those school.

Montana

In September, the Columbia Falls School district in Montana closed more than 30 schools for three days after the Dark Overlord stole data from the district server. Police called the hacker a "cyber terrorist."

By Sept. 13 and 14, parents were receiving "extremely graphic threats via text messages." After a reporter asked why the Dark Overlord targeted Flathead Valley, the hacking group replied, "I wanted the public to exist in a state of fear before I make my move. This will allow the government protecting your children to look poorly in the light of the public. … The quaint, small, backwoods region of the US like yours is prime hunting grounds. This incident is the last thing you will expect to happen here."

The school district received a seven-page ransom letter (pdf) demanding $150,000 in bitcoins on Sept. 18. Two of the three payment options offered "significant" discounts if the associated demand was met.

Texas

Also in September, Splendora School District in Texas was hacked and students' personal information was compromised. Although the school district did not release any potential ransom demand it had received on Sept. 27, it did put out a statement on Sept. 29:

"We continue to receive threats from the group/individual responsible for hacking our network. They have threatened a tiered escalation which could include direct messages to parents, students and staff. We do not know the exact information that they have, but it could contain specific names and confidential information, such as phone numbers and addresses. In previous cases, these messages have been via text and/or email, and have been violent and graphic. The point of this is to incite fear and panic for parents."

Parents were told not to engage the hackers and to send a copy of any threatening text or email to the police. The school district did not name the Dark Overlord in the statement, but after school officials contacted the Montana school district that was attacked, Columbia Falls Superintendent Steve Bradshaw said, "They believe the case is similar."

HackRead reported that, like in Iowa, the details of the Texas and Montana school hacks were published on Pastebin.

Alabama

Crenshaw County Schools in Alabama shut down for two days last week, on Oct. 3 and Oct. 4 after the FBI notified the school about a "threatening social media post." It seems unlikely to be related, as there was no mention of parents receiving threatening text messages or of The Dark Overlord, but an article from the hack in Montana suggested it was a similar incident.

If a person threatens you, that's one thing. But if a person threatens your kids, that's an entirely different matter. Schools had better get on it and batten down the security hatches because there is no excuse for their lax security. There may be limited money in the budget for security solutions, but they can at least keep devices patched. If the threat of being hit with ransomware doesn't prod school districts to clean up their sloppy security, let's hope protecting kids and their parents from threats will.

Return to Motivations for Social Engineering

Nigerian Email Scammers Are More Effective Than Ever

WIRED | Lily Hay Newman | 05.03.18 | 08:00 am

You would think that after decades of analyzing and fighting email spam, there'd be a fix by now for the internet's oldest hustle—the Nigerian Prince scam. There's generally more awareness that a West African noble demanding $1,000 in order to send you millions is a scam, but the underlying logic of these “pay a little, get a lot” schemes, also known as 419 fraud, still ensnares a ton of people. In fact, groups of fraudsters in Nigeria continue to make millions off of these classic cons. And they haven't just refined the techniques and expanded their targets—they've gained minor celebrity status for doing it.

On Thursday, the security firm Crowdstrike published detailed findings on Nigerian confraternities, cultish gangs that engage in various criminal activities and have steadily evolved email fraud into a reliable cash cow. The groups, like the notorious Black Axe syndicate, have mastered the creation of compelling and credible-looking fraud emails. Crowdstrike notes that the groups aren’t very regimented or technically sophisticated, but flexibility and camaraderie still allow them to develop powerful scams.

“These guys are more like a crew from the mafia back in the day,” says Adam Meyers, Crowdstrike's vice president of intelligence. “Once you’re in an organization and are initiated, then you have a new name that’s assigned to you. They’ve got their own music, their own language even. And there are pictures on social media where they’re flaunting what they’re doing. The whole idea is why invest hundreds of thousands of dollars to build your own malware when you can just convince someone to do something stupid?”

Yahoo Boys

Young Nigerian scammers have often been called “Yahoo Boys,” because many of their hustles used to target users on Yahoo services. And they've embraced this identity. In the rap song “Yahooze”—which has more than 3 million views on YouTube—Nigerian singer Olu Maintain glamorizes the lifestyle of email scammers.

'They spend months sifting through inboxes. They’re quiet and methodical.' James Bettke, Secureworks

Advanced Nigerian groups have lately increased the amounts they make off with in each attack by targeting not just individuals but small businesses. The FBI estimates that between October 2013 and December 2016 more than 40,000 "business email compromise" incidents worldwide resulted in $5.3 billion in losses. With so many many third parties, clients, languages, time zones, and web domains involved in daily business, it can be difficult for a company with limited resources to separate out suspicious activity from the expected chaos.

Nigerian scammers will send tailored phishing emails to a company to get someone to click a link and infect their computer with malware. From there, the attackers are in no hurry. They do reconnaissance for days or weeks, using key loggers and other surveillance tools to steal credentials to all sorts of accounts, figure out how a company works, and understand who handles purchasing and other transactions.

Eventually the scammers will settle on a tactic; they may impersonate someone within the company and attempt to initiate a payment, or they might pretend to be a company the victim contracts with and send the target an innocuous-looking invoice to pay. If they've gained enough control of a system, attackers will even set up email redirects, receive a legitimate invoice, doctor it to change the banking information to their own, and then allow the email to reach its intended recipient. And the scammers rely on this sort of man-in-the-middle email attack for all sorts of manipulations.

Even though the attackers generally use cheap commodity malware, the groups tend to remain inconspicuous on victim networks, and have shown a willingness to abandon ideas quickly if they're not working. One technique called "domain tasting" involves registering domains that look legitimate, trying to send phishing emails from them, and then moving on to a new domain if the phishes aren't working.

"It's malware and phishing combined with clever social engineering and account takeovers," says James Bettke, a counter threat unit researcher at Secureworks, which has tracked Nigerian email scammers for years. "They're not very technically sophisticated, they can't code, they don't do a lot of automation, but their strengths are social engineering and creating agile scams. They spend months sifting through inboxes. They're quiet and methodical."

In one case, Bettke says, scammers used their position impersonating an employee at a company to brazenly ask their target for the organization's official letterhead template. In other situations, scammers will make Skype video calls to legitimize transaction requests, and use a still from a video they find of the employee they are impersonating to make it seem like the person is genuinely calling and the video is just lagging behind the audio. After victims wire their money away, the scammers often route it through China and other Asian countries before moving it a few more hops and landing it in Nigeria.

"It's a simple approach and it works," Crowdstrike's Meyers says. "They target organizations' payroll, accounts payable, they'll claim to be a vendor. And then they do a phone call or something else to the victim to increase the credibility of the scam."

Social Engineers

The groups often aren’t very careful about covering their tracks They'll brag on social media under Confraternity pseudonyms about their crimes, trade tips on Facebook groups that can be infiltrated, or purchase flawed malware that ends up exposing their movements. Often, even if they make an effort to delete signs of their intrusion on a network, analysts will still be able to trace malicious traffic back to Nigerian IP addresses, and the scammers generally don’t have proxying protections in place.

Law enforcement groups around the world, including the FBI, Interpol, and Canadian and Italian agencies, have successfully indicted and arrest various kingpin scammers. But extensive jurisdictional issues make it an especially difficult problem for law enforcement. And many victims have little recourse once their money is gone.

“When a small business gets scammed out of $200,000 or $500,00 they’re just done, they’re no longer in business,” says FBI agent Michael Sohn of the Los Angeles Cyber Division. “So we’re working with banks to recover funds when possible, and also with private sector companies and security companies to share intelligence. For victims it’s heartbreaking, it’s just absolutely devastating.”

'These guys are more like a crew from the mafia back in the day.' Adam Meyers, Crowdstrike

While Nigerian email scammers take a different tack than hacking groups in Eastern Europe and Russia, researchers say they still pose a genuine threat. “What stands out about this community of criminals is their willingness to learn from each other, and a near myopic focus on social engineering scams,” notes Mark Nunnikhoven, the vice president of cloud research at TrendMicro, which collaborates with Interpol and other law enforcement agencies on tracking Nigerian email scammers. “These two traits have led to a rapid increase in sophistication of the criminal schemes.”

Researchers say that businesses should try to protect themselves with basic steps like updating software and adding two-factor authentication, so even if scammers steal account credentials they can't wreak instant havoc. Adding administrative controls to limit the types of emails and attachments employees can receive can also screen out some phishes, and adding an indication when messages come from outside the company's own email domain can help flag malicious emails pretending to be from a colleague on a similar-looking server.

Crowdstrike's Meyers also suggests that small businesses set requirements that multiple people sign off on large transactions. "It's like in nuclear missile silos where two people bring the keys," he says. "It's possible for one person to get duped but harder for two." Still, when hackers know everything about who you are and how you work, there's only so much you can do to stop them.

Return to Motivations for Social Engineering

Resist Phishing Attacks with Three Golden Rules

WIRED | Lily Hay Newman |12.09.17 |06:00 am

That sense of urgency, or that threat from an authority figure, or that random ask for help, all conspire to force you to click. Aaron Fernandez

Like any classic hustle, phishing has staying power. The fake emails and texts that lure you into a digital con—*Free cruise! Act now!*—may not comprise a very technical hack, but the attackers behind them still put a lot of resources and expertise into giving their cons as much authenticity as possible.

That's what makes it so difficult to protect yourself against phishing. You know not to click links in shady emails. You know to think twice before clicking *any* link in *any* email. (Right?) The same goes for downloading attachments and putting your personal information or login credentials into any form that you have any reason not to trust. And yet! Phishers can just needle you forever, waiting for that one moment when you finally slip up. If you do, you instantly subject yourself to any number of unfortunate consequences, whether it's identity theft, fraud, or malware that runs rampant on your device.

Follow these three rules to keep from getting hooked.

Rule 1: Use Context Clues

The best way to spot a phishing scheme is to listen to your gut. Remember, even if an email looks like it comes from a friend, that doesn't mean it's safe. If you weren't expecting an email from someone, or if you were but the email seems rushed, or their tone is off, or they're sending you a Facebook message when they usually text you ... If anything seems even a little bit off, check with the purported sender on another platform to confirm that they actually reached out.

If a message comes from a person or entity you *don't* already know, consider the context of why you might be receiving it and whether the message really makes sense. Most online services won't, for instance, appear out of the blue, asking you to make account changes through an email link. And even if they do, you should always navigate to the site separately, log in, and check to see what's actually going on. Treat attachments with even more suspicion and avoid opening them altogether, particularly if you didn't ask for them or didn't have a pre-arranged plan to receive them.

Rule 2: Remember the Basics

Following standard digital defense advice will help with phishing as well. Keep a backup of your data. Enable multifactor authentication on every account that offers it. Close accounts you don’t use anymore. And set up a password manager to keep track of unique, robust passwords. All of these steps make you a tougher target, but more importantly, they'll help contain damage if you ever do get phished.

Rule 3: Know Thyself

At its core, phishing defense requires an awareness of the human traits scammers prey on. “The thing I find fascinating about phishing is it’s really exploiting a very primal part of human behavior,” says Crane Hassold, a threat intelligence manager at the security firm PhishLabs, who previously worked as a digital behavior analyst for the FBI. “It’s all about curiosity, trust, and fear. Those qualities are really hardwired into humans, so a lot of protection against phishing has to do with conditioning yourself to look out for things that could be a red flag.”

This means being in touch with your instincts and emotions as you read your messages. That sense of urgency, or that threat from an authority figure, or that random ask for help, all conspire to force you to click. You need to recognize those emotions before acting on them and consider the possibility that a message has nefarious reasons for trying to elicit them. It’s time to really internalize a hard truth: No one is ever going to give you free cruise tickets. Truly never.

Return to Motivations for Social Engineering

Three Hackers Plead Guilty to Creating IoT-based Mirai DDoS Botnet

CNET | Alfred Ng | December 13, 2017 8:08 AM PST

Three hackers have admitted to building the tools that attackers used to take down many of the internet's most popular websites.

Paras Jha, 21, pleaded guilty to multiple charges related to creating and operating the Mirai botnet, according to federal indictments unsealed Tuesday. His partners, Dalton Norman, 21, and Josiah White, 20, pleaded guilty to conspiracy to violate the Computer Fraud & Abuse Act.

Jha admitted to writing the source code for Mirai -- malware that created a botnet that took over hundreds of thousands of computers and connected devices like security cameras and DVRs -- and using it to commit attacks and online fraud. Norman also admitted to helping write the code, as well as directing click fraud and online attacks.

None of the botnet's creators were responsible for the attack that took down popular websites in October 2016, the FBI told Wired. Their initial motivation was to attack servers running the popular online game Minecraft, according to Wired. Security writer Brian Krebs first identified Jha and White as the programmers behind the botnet -- and their interest in Minecraft -- in January.

White told prosecutors he created Mirai's scanner in August 2016, which scoured the web for vulnerable devices the malware could hijack. He also hosted the servers on which the malware operated and hijacked a computer in France in an attempt to disguise the source of the attacks.

"The Mirai and Clickfraud botnet schemes are powerful reminders that as we continue on a path of a more interconnected world, we must guard against the threats posed by cybercriminals that can quickly weaponize technological developments to cause vast and varied types of harm," Acting Assistant Attorney General John Cronan said in a statement.

The attack that took down Twitter, Netflix, Reddit, Pinterest and several others came in 2016, after the botnet -- Mirai's army of hijacked machines -- set its targets on Dyn, an internet management company based in New Hampshire. The websites relied on Dyn to direct traffic, and the attack sent a massive amount of traffic to Dyn's servers in a Distributed Denial of Service attack, also called a DDoS attack.

Prosecutors said Jha sold the botnet to other criminals online and threatened companies with similar DDoS attacks unless they paid up. From September to October 2016, Jha made Mirai's source code public on forums for cybercriminals, allowing anyone to use it.

Jha maintained the botnet, which hijacked more than 300,000 devices, while looking for new victims to attack and infect, according to court documents. The attacks caused at least $5,000 in damage.

New Hampshire Sen. Maggie Hassan, a Democrat who's been vocal about the need for increased cybersecurity regulation, praised Justice Department but also cautioned that more needs to be done.

"I am pleased that justice has been served," she said, "but there is much more work to be done to defend against cyberattacks of this kind and to secure the Internet of Things."

They also plead guilty to creating the Clickfraud botnet, which flooded traffic to websites and raked in cash from online advertising. The scheme netted Jha and his crew nearly 100 bitcoin, which was valued at $180,000 on Jan. 29. It's now worth more than $1.7 million.

As part of Jha's plea agreement, he'll have to give up 13 bitcoin to the US government, currently valued at about $226,500. White is giving up 33 bitcoin, valued at $571,000. The attackers each face up to five years in prison and a fine of at least $250,000 for their involvement with the Mirai botnet.

Jha also pleaded guilty in New Jersey to violating the Computer Fraud & Abuse Act for launching an attack on Rutgers University's network using the Mirai botnet. Jha, a former student at the New Jersey school, admitted to shutting down servers that students, faculty and staff used to turn in assignments.

The attacks lasted for several days and affected tens of thousands of students, said William Fitzpatrick, acting US attorney for the district of New Jersey, in the release. Jha faces an additional 10 years in prison and a $250,000 fine for his attack on the university.

Return to Motivations for Social Engineering

Revenge Hacks Cost Former Employee 34 Months in Prison, $1.1 Million in Damages

BleepingComputer | Catalin Cimpanu | February 17, 2017 | 11:46 AM

Brian P. Johnson, 44, of Baton Rouge, Louisiana, will have to spend the next 34 months in federal prison and pay $1,134,828 in damages after hacking his former employer shortly after being fired.

According to court documents, Johnson worked for several years as an IT specialist and systems administrators for Georgia-Pacific, a company that describes itself as one of the world's largest manufacturers of paper, pulp, tissue, packaging, building materials, and related chemicals.

On February 14, 2014, management at Georgia-Pacific's Port Hudson mill terminated Johnson's contract, and security escorted Johnson out of the factory's premises.

Johnson hacked his former mill, affecting production

Holding a grudge for his sudden termination, investigators say that during the next two weeks, Johnson used his previous accounts to connect to the mill's network and alter various configurations, bringing, in some cases, the mill's production to a halt.

Suspecting that Johnson may have been behind some of the attacks, Georgia-Pacific requested the FBI's assistance, which on February 13, 2014, executed a search warrant at Johnson's house.

Investigators weren't wrong, as court documents reveal that FBI agents found an open virtual private network connection to Georgia-Pacific's network on Johnson's computer screen when they searched his home in Zachary, Louisiana.

Following a thorough investigation of Johnson's remote sessions to the Port Hudson mill after his termination, FBI agents concluded that the former employee intentionally sabotaged his former employer as payback.

Johnson now has to pay over $1.1 million in damages

A year later, in February 2016, faced with all charges, Johnson formally admitted his crimes. Following his guilty plea, a judge sentenced him to two years and ten months in prison, and also awarded Georgia-Pacific damages to cover the downtime brought by Johnson's hacks.

According to its homepage, Georgia-Pacific employs about 35,000 people in more than 200 facilities, and its mills run around the clock, meaning any downtime resulted in setbacks.

Johnson is not the first or the last employee to hack his former employer. Last year, a sysadmin who worked for a Pennsylvania ISP received two years in prison for crashing the ISP's network and then requesting a ridiculous sum of money to help fix the problem.

Return to Motivations for Social Engineering