nLightenedThoughts

March 2017

William Blinn Communications
Worthington, Ohio 43085
www.blinn.com • 718.577.1054

Providing an Outstanding Experience for Clients

No matter what you do, the least positive experience might be the one that people will remember. It's not inevitable, though. You can change what's remembered and here's how.

Recently I blundered across "Understanding Micro, Macro, and Meta Experiences, A New Way of Looking at Experience Design" by Laurence Bernstein, Managing Partner, Protean Strategies, in a publication for hotel managers. I don't own or manage a hotel. You probably don't, either, but there's some useful information here.

Bernstein says there are three classes of experiences: micro, macro, and meta.

The goal is to provide clients with an experience that is so positive that they become evangelists. As Bernstein explains, "for the most part guests don't return to any single city all that often, but they have friends that visit and their friends have friends."

Bernstein describes two scenarios. These are, of course, specific to hotels, but you can easily imagine an equivalent event in your line of work.

Scenario 1: A guest stays in a hotel and everything is perfect. In other words, the check-in is quick and easy, the room is clean, everything works, all the employees smile. That's great, but there's no overwhelmingly superior experience. "If asked, they would probably say the hotel was nice, or fine, or okay, and little else." Nothing memorable.

Scenario 2: Everything is identical to scenario 1 except this: At breakfast on the day the guest is checking out, a waiter accidentally spills coffee on the guest. That one event will have changed their overall perception. "When asked, they will always tell the story of the careless waiter who 'ruined their experience.' Even if the hotel was the most flawless operation in the universe, they would have nothing else to talk about, because the only memorable experience — the only experience that stands out — is the burning coffee."

Bernstein says that he worked for several years at a premier hotel in Vienna. The guests who stayed there became evangelists for the hotel. "They never mentioned the frayed carpets or the lack of air conditioning or the slow elevators." Instead, Bernstein writes, they based their positive reviews "on a few outstanding services and amenities, and the generally good feeling they had about the place when they left."

Managers of the hotel in Vienna worked hard to ensure that the guests had several positive memorable experiences and no negative memorable experiences. Take the incident of the spilled coffee. It happened at the end of the guest's stay, so it had no effect on the rest of the stay — yet it's the event the guest will remember, the event that the guest will believe spoiled the entire trip. That can be fixed, though, and we'll see how in a bit.

Bernstein writes, "For an experience to become a 'remembered' experience it needs to be relevant and salient. That is, it must be of interest in one way or another to the experiencer and it has to stand out from other experiences in one way or another."

That leads to the three types of experiences.

Micro, Macro, and Meta

Not all experiences are equal and Bernstein recommends categorizing them as micro, macro, and meta experiences.

"Micro experiences are the uncountable number of events or activities we experience; macro experiences are those that for one reason or another have a degree of salience that causes them to stand out from the micro experiences; and meta experiences are the aggregated experience of all the macro and micro."

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, Worthington, Ohio.
Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com. All rights reserved.

In a rain storm, individual rain drops would be the equivalent of micro experiences. Individually they have little effect, but there would be no storm without them. For a hotel, these would include things like the revolving door, the fan in the elevator, the lights in the hallway — all essentially invisible unless there's a problem with them.

A macro experience in the rain storm might be the result of an impressive lightning bolt, particularly if it strikes nearby.

For example, I recall a lightning bolt that hit nearby when I was driving. It happened in the late 1980s. The lightning bolt hit so close that it knocked out the radio in my car. I remember the part of town I was in, too, and that was more than 25 years ago!

The spilled coffee incident is a macro experience and it will be negative *"unless there is a really brilliant recovery by the hotel management, which, coming as it would at the very end of the experience, would be like the rainbow at the end of the storm: the most remembered experience that defines the ultimate outcome as beautiful!"*

All experiences roll up into the meta experience, "the experience of all experiences" — or the final remembered experience that "becomes the filter through which all experiences, good or bad, will be viewed and recalled."

Meta Experiences Count

THE BOTTOM LINE: "IN THE END, IT'S NOT WHAT YOU DO; IT'S NOT WHAT GUESTS REMEMBER YOU DO; IT'S NOT EVEN WHAT GUESTS IMAGINE YOU DID: IT'S WHAT GUESTS DECIDE TO THINK ABOUT WHAT THEY THINK YOU DID."

If that seems a bit convoluted, you're right. Bernstein goes on to say that thinking of ways to ensure guests are feeling positive at the end of their stay will result in positive memories of specific experiences.

In that regard, it's a situation any marketer or business owner will recognize as the universal question from clients and customers: "What have you done for me *lately*?"

If you'd like to read the full article, you'll find it on the Hotel Executive's website. *http://hotelexecutive.com/business_review/4431/understanding-micro-macro-and-meta-experiences* (Short link: *goo.gl/okWOQN*) Ω

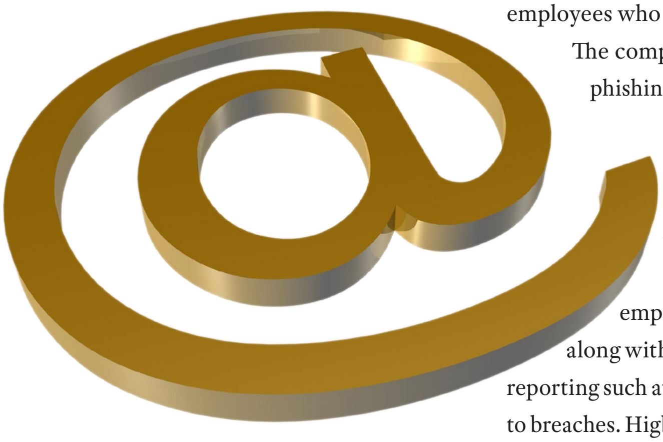
Cyberattack Common Vector: Email

EMAIL IS ESSENTIAL, BUT IT'S ALSO THE MOST COMMON WAY THAT MALWARE IS INJECTED INTO CORPORATE COMPUTER SYSTEMS.

More than 90% of attacks start with email and many of the messages use some sort of social engineering. No matter how much security experts preach "don't click that link", people still do. Research conducted by PhishMe examined why people click these links: The top 3 reasons are curiosity, fear, and urgency. The other reasons the victims cited were reward, recognition, entertainment, and opportunity.

According to PhishMe co-founder Aaron Higbee, employees who are pushed to perform their jobs quickly tend to be more likely to click a fraudulent link if there is an element of urgency in the message. The need to act quickly plays into the hands of criminals, Higbee says, because employees fear job loss if they don't work fast.

PhishMe's approach is unusual: After being hired, the company sends phishing messages to everyone in the company. The messages contain no malware. They're simply intended to identify those employees who click fraudulent links.



The company sent some 40 million phony phishing emails to about 1000 companies. In the insurance industry, about one third of the recipients clicked on the bad links. Retail, energy, and healthcare did slightly better.

Training is the key to improving employee understanding of the threat along with instilling an understanding that reporting such attempts can ensure faster response to breaches. Higbee says that prompt reporting can reduce the amount of time required to discover a breach from months to less than a day.

If your company has 25 employees, that's 25 potential attack vectors. 100 employees offer 100 possible targets. The scammer needs to convince only one person to click a bad link and someday you or one of your employees *will* make a mistake.

The more important consideration, then, is determining how to limit the damage.

Network segmentation is relatively inexpensive to implement and it can be used to limit access to the company's most valuable resources. Not everyone in the business needs access to the accounting server, for example. In a retail operation, point-of-sale devices should be isolated from the rest of the network. A security expert can make recommendations that are specific to your operation.

It's also important to teach people to respond quickly. Make sure they understand that there will be no punishment for accidents, but that they need to be reported immediately. The longer malware is active on the network, the more harm it will do.

Nearly 20 years ago, I mistakenly clicked a bad link and realized immediately that there was a problem. After disconnecting my computer from the network, I notified the company's security officer. Damage was limited to files on my computer because I had taken it off the network and clean-up was much easier than it might have been.

So although training people to recognize and avoid malware it good, it's also essential to train them to sound the alarm when something bad happens, just as all good employees would do if they noticed a small fire burning in the corner. If you wait, the problem won't go away. Ω