

Of ATMs and Phishing

By Andy Cottrell

Imagine you open the newspaper to read that a large number of ATM machines in your city are actually completely fake. That when used, they will steal your deposits and your ATM cards and PINs. As quickly as your local bank finds and shuts down these fake ATM machines, new fakes spring up. And worse, your bank tells you that you if you lose your money to such a machine, you are out of luck.

The consequences would not be hard to imagine:

- ▼ The bank and consumers lose money as the stolen ATM cards/PINs are used at genuine machines.
- ▼ Consumers would stop using ATM machines as they would be unable to tell the genuine article from the fake.
- ▼ Consumers would, however unfairly, cast their ire on the bank.
- ▼ The bank might in turn, however unfairly, be irritated that customers are not more careful about where they insert their ATM card.
- ▼ Upper management would immediately blame IT security for failing to prevent this turn of events.

Luckily for the world of ATMs, incidents of criminals creating entirely fake ATM machines have been rare (though they have happened!). Unluckily for on-line financial services, the on-line equivalent, also known as phishing, is now rampant. Phishing, as many of you already know, is an on-line scam in which an e-mail is sent to a user falsely claiming to be from an established legitimate enterprise. The e-mail is an attempt to trick the user into surrendering access information the thief can use to steal from the user's account or personal information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to enter information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Because phishing scams play off the trust a user has with the institution he/she *thinks* it is interacting with, it has been remarkably effective, and phishers have been quick to evolve their tactics as enterprises fight back. As security professionals, we are on the front lines of solving this problem.

Solving the Problem

As it turns out, strategies to combat on-line phishing are not very different from how we would combat the fictional scourge of fake ATM machines. We would, as a first line of defense, try and educate customers so that they could tell genuine ATM machines from the fake ones. For example, train customers to only go to ATM machines attached to bank

branches or to watch out for ATMs with misspellings on the screens. And we would try and tear down the fake machines as soon as we find them.

Unfortunately, in the on-line world, this strategy is proving of limited value, as the phishers rapidly adapt, and are able to produce digital copies of e-mail communications and Web sites that are virtually indistinguishable from the real ones. And emerging threats like pharming, where the phisher attacks a DNS cache, make it virtually impossible for even the most conscientious and knowledgeable user to completely avoid falling prey to a fake Web site. With pharming, typing the correct URL directly into the browser will still take you to the phishing site, since the local Domain Name Cache has been tricked into sending you there. This does not mean that the first line of defense has no value; it simply means that it is by itself insufficient.

A slightly more powerful defense would be an ATM card where the PIN changed with each use. If an attacker with a fake ATM stole the card and the PIN, they get only one try at using it at the genuine site. Unfortunately, "one try" might be all they need to steal all your money, so this defense does not help too much by itself. The one-time password-based tokens of the on-line world are not without value, but they need to be used in conjunction with other methods.

What would be a more powerful defense? Returning to our fictional example, what if we could design ATM cards that would only slide into the slot of a genuine ATM machine? In other words, it would be impossible for a user to give up their authentication credential even if they are completely fooled by the appearance of a fake ATM machine!

Strong Authentication

While we do not know how to design such ATM cards, as it turns out, such credentials do exist in the on-line world to allow users to authenticate to Web sites. We call such authentication "strong authentication." We do observe that there is no industry standard for what "strong" authentication means, how it is deployed, or what it looks like to users, but what it does is provide a credential that you simply cannot give away to an attacker.

So why is everyone not already using such "strong" authentication? The primary reason is that the first generation of such products were high on security, but were frankly way too costly and cumbersome. While our fictional bank was upset with the fake ATM machines, would they have deployed an ATM card that cost the bank \$1,000 per card? Would consumers have adopted a secure card that weighed 30 lbs?

But we do not have to give up on "strong" authentication. Emerging technologies are in fact solving the problems inherent in first-generation technologies that focus on three innovations:


1. These solutions recognize that great security by itself does not suffice; it must be tightly integrated with end user convenience and realistic deployment costs.
2. They recognize that there is no "one size fits all." To continue our ATM card analogy, different users might need ATM cards of different strengths (and with different usability and cost considerations). However, just because we have 'ATM cards' of different strengths does not mean we can afford multiple "ATM machines" for each strength, at every location. Rather, the same ATM machine should service all these different types of 'cards.' IT security budgets, although increasing a few percentage points a year for the last ten years, have certainly not kept pace with the threat environment. Even if your budget has doubled, what is the increase in threat? 100 times? 200 times?
3. They cleverly blend the best features of multiple authentication technologies—such as zero footprint cookie-based, device authentication, one time passwords and smartcards—to create a smorgasbord of options. This allows a financial institution to address the needs of all its consumers, ranging from those for whom the convenience of password-only based access is paramount, to those for whom a stronger second factor—such as a smart card or USB token, is well justified.

Let's examine in more detail how these solutions can help with our phishing problem. No doubt you have already divided your user base into low risk, medium risk and high risk, or similar tiers. For low-risk users, particularly customers on unmanaged machines, a zero client footprint, cookie-based solution will defeat many types of phishing attacks without causing user inconvenience. In our ATM analogy, the user's ATM card looks as it always has, but has a special encrypted file that only a real ATM can read. The ATM can now recognize the user when the card is inserted and provide feedback (information that only the bank knows) on the screen to assure the user this is a "real" ATM before the user types in the PIN. In addition, if that special file is missing, the ATM knows to be suspicious and ask for additional authentication information before providing access.

Another option would be to allow the ATM card to authenticate the ATM and vice versa before it could be inserted. The Internet version of this is turning on client authentication in SSL. The ATM card would "refuse" to speak with the fake ATM, since it would not be able to authenticate it. The user could then take the card to another machine. This option could be used for higher-risk customers, maybe those who travel and can't always find a local bank branch with an ATM.

Conclusion

When choosing the type of protection to implement, also keep in mind the wide variety of phishing and pharming attacks, as well as the inevitability that the attackers will constantly think up new ways to separate your customers and your business from their money. The new technologies on the market also give you the ability to migrate users to stronger protection over time.

With the availability of these practical, real world, strong authentication options, the path forward is clear! As IT security experts, it's our responsibility to provide as much protection for users and the enterprise as possible. 

Andy Cottrell is CTO of TriCipher.