



Selecting a phishing prevention solution: six key questions

Is it really a phishing prevention solution?

Many products in the anti-phishing space are forensic; they offer phishing detection, not phishing prevention. Some of these can be great as part of a layered anti-phishing strategy. But here's a critical question: will the solution prevent phishing attacks from happening at all, or will it merely report that your online service is being, or has already been targeted in a phishing attack?

Is it visible to the user?

The main threat to business from phishing is not direct losses; it is the reputation or brand damage that can result from negative publicity. Research shows that concerns about security are amongst the main factors preventing users from doing more business online. Worse still, media reports of service providers being phished can cause existing online consumers to stop doing business online or even to change to another brand if it is perceived to offer better online security. Increasing the actual security of an online service is important, but unless some of the security enhancement is made visible to users, the main issue will remain unaddressed, namely user confidence.

Does it rely on user good behaviour?

Social engineering phishing works by tricking users into willingly disclosing their login credentials on fake websites. Once disclosed, a password remains forever compromised. Some users may disclose their login credentials because of lack of awareness, but research has shown that the best visual deception phishing attacks can fool even the most sophisticated users. One response is to urge users not to enter their credentials unless they see the website displaying text or images they have previously selected, thereby validating that the website is authentic. Unfortunately, the first independent study of this class of solution demonstrates that absence of pre-stored site authentication elements constrains user behaviour in less than 10% of cases. Asking people to 'be careful' is not a good or reliable defence against well-executed confidence tricks!

Is it self-explanatory?

It is not difficult to design and implement a truly secure authentication solution, but the challenge is to make it usable by real people, especially for mass-market, consumer-facing services. Great design is self-documenting – how to use the product will be immediately apparent from its design properties, eliminating the need to read a manual or attend a class to start using it. This should be true of phishing prevention login solutions – if user adoption requires significant user training or support it's probably the wrong solution.

Does it defeat Trojan viruses?

Trojan viruses represent the fastest growing variety of phishing. If user identity credentials can be captured by malicious spyware on input, then they are vulnerable. At present, almost all authentication methods in which the user's login credentials are typed are at risk from keystroke logging Trojans.

Is it a zero-footprint solution?

Some anti-phishing solutions require users to be in possession of security components, such as password-generating tokens, one-time password pads, or client software installed on access devices. These can have a substantial impact on the cost, operational logistics, and user acceptance of the solution. To optimize these, a zero-footprint solution should be selected, i.e. one implemented 100% on the server side, with no requirement for users to have anything special in their possession or installed on their PC at login time.