

Predictions for the New Year

Now is that time of year where "experts" are asked to weigh in with predictions for next year. As one of these so-called experts, I will agree with the timeless adage that there is nothing new under the sun. While this is not exactly true from a security standpoint, it could not be more accurate. I don't see any significant changes. I could wax eloquently about what we already see and pretend that they are new trends, but in all honesty, not much is going to change significantly. If you follow the trends then you are going to be a victim. Security requires planning and plugging holes proactively.



Randy Abrams

The major "new" avenue of attack will be the exploitation of legitimate websites. If the bad guys can get their software onto a legitimate website, it will be very easy to infect the computers of unsuspecting users. This is not a new trend, back in 2007 the Miami Dolphins' Super Bowl website was compromised and many people who visited the site got infected. Savvy users know to stay away from suspicious websites, but rarely suspect that legitimate sites might infect them. This attack is very effective when social engineering fails.

Simply stated, social engineering is the art of getting someone else to do what you want them to do. These attacks are common and increasing in frequency. The attacks take many shapes. Phishing attacks are one form of social engineering. Emails that claim to be greeting cards or links to porn are another type of social engineering attack. Attacks directed against employees of companies in order to gain access to confidential information are becoming more common. Telephone calls are now being used by criminals who pretend to be from banks, etc. In reality this type of attack has gone on for years, but is becoming increasingly common as more criminals learn they can use voice over IP to make effectively untraceable calls.

The security trends of the New Year are simply a continuation of what we have been seeing. The wise employer trains its employees to avoid social engineering. There is not a lot that can be done to protect against legitimate websites, at least not cheaply. That said, security is about managing risk. We do not eliminate risk. People would like to think their security software can completely eliminate risk, but it simply is not the case. Well trained users coupled with layered security are the best defense in the Internet age.

The user who makes a New Year's resolution to learn more about security will be the one who will have fewer security problems next year.

If you wish to submit questions or comments to "Ask the Expert" please feel free to send them to askeset@eset.com.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.