How Unlikely?

Suppose an event was considered very unlikely, like someone guessing an 8 digit number. The probability that a single random guess is correct is 1 in 100 million. If we don't repeat bad guesses, then the expected number of random guesses needed before getting the correct number is about 50 million. So, if we guessed 1 number per second, every second, we would expect that it would take (on average) about 579 days before the correct number was hit. Of course, if you want to be sure that the correct number gets hit, then you would need to budget for the worst case of about 1157 days (the correct guess didn't get hit until after all other $99,999,999$ possibilities were tried).

Suppose we are selecting from a sample of n labeled elements, and one is "correct". We select ("guess") until we select the correct element. That the expected number of guesses before success is about $n/2$ makes sense; in fact it is exactly $(n+1)/2$: If there are 2 elements, then the possible (and equally likely!) outcomes are {right} and {wrong,right}. If $n = 3$, then the possible outcomes are {right}, {wrong,right} and {wrong,wrong,right}. For $n = 2$ the average number of guesses is the mean of $\{1, 2\}$. For $n = 3$ the average number of guesses is the mean of $\{1, 2, 3\}$. If you hypothesize that the expected number of guesses before success is the mean of $\{1, 2, \ldots, n\}$, then you are right, and that mean is $g(n) = (n+1)/2$.

Now suppose we have some feedback. For example, suppose that we guess the 8 digit number one digit at a time, *and we are told whether that digit is wrong or right.* Then we have broken our problem into a process consisting of 8 steps, each of which is to correctly guess one of the numbers $\{0, 1, \ldots, 9\}$. What is the expected number of guesses needed before getting the correct number now? Well, since there are 10 elements in $\{0, 1, \ldots, 9\}$, we expect that it will take, on average, $g(10) = 11/2$ guesses per digit, giving a grand total of $8 * 11/2 = 44$. Yes, on average, only 44 guesses will be needed to guess this 8 digit number! With feedback we can do in about 44 seconds what it took about 1.5 years to do without! With feedback, the worst case takes 80 seconds (each digit takes 10 guesses), compared to over 3 years without.

Of course this can be generalized. I can guess a random (English) 4-letter string on average in 228,488.5 guesses, but with letter-by-letter feedback it only takes an average of 54 guesses. Is this how safe-cracking works? (I don't know). Did you ever play "20-questions"? This feedback is certainly *not* possible in standard software for passwords, PINs, etc. Feedback may or may not be present in a given natural system, but when it is evident, we should not be surprised by that system's complexity nor impressed by its "improbability".

In fact we *should be* very surprised to find *any* biological system without many and various kinds of feedback. The most fundamental type of biological feedback is probably:

"if you have no offspring, then you don't pass your genes on"...