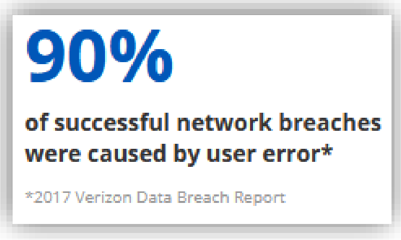
BUILT ON IT

# Security Awareness Training

## Overview:

Cybersecurity awareness has become key in reducing the number, frequency, and impact of IT Users being the conduit for IT Security breaches. Cybercriminals today auto-research and target individuals in bulk as an easy entry point into organizations' systems, which is far easier than writing a software exploit or finding ways to bypass IT Security defences.

User education via cybersecurity awareness training is, if conducted and managed properly, a highly effective way of arming users against the would-be social engineering hackers. At the same time, it helps foster good IT habits like password management, locking work stations, and other IT security habits and practices that make IT a lot safer.



**90%**

**of successful network breaches were caused by user error***

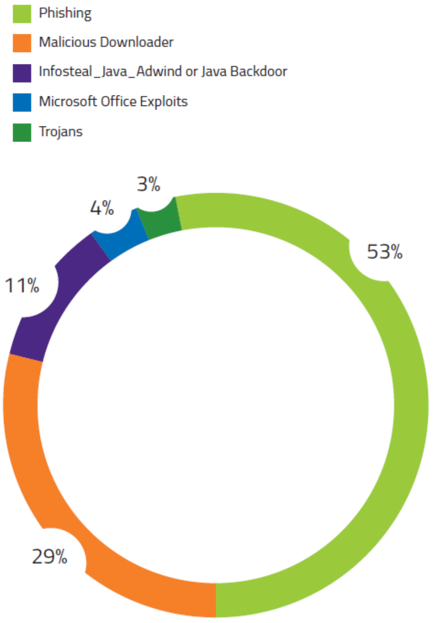
*2017 Verizon Data Breach Report

## Effective SAT (Security Awareness Training):

The effectiveness of any user education training is based on it being something you can measure over time. To achieve this, it needs to be run continuously so the results from individual users can be compared over the entirety of a program. This then allows the organization to see if the desired changes in behaviour are being achieved, or other courses of action are needed to reinforce or accelerate that change.

A key goal is to foster interactivity from within the computer-based training. This interactivity can take many forms, but is essential, as it allows the user to become more involved in what is being communicated, and it often takes the form of tests and quizzes to determine how much individual participants are absorbing from the education courses.

Webroot brings all of these to bear in its Security Awareness Training campaigns and ongoing user education programs — continuous, relevant, and involving education campaigns that together create an education program tailored to the IT users' role.



Top attacks detected by Microsoft Office 365

*Powered By:* WEBROOT Smarter Cybersecurity

## Features

- Phishing Simulator with expanding real-world template library.
  Phishing is the primary way users are socially engineered. Our ever-expanding and topical phishing template library is regionalized for effectiveness and relevance, while allowing realistic engagement with IT users in real-world phishing scenarios.
  Launching realistic phishing attack simulations lets you accurately monitor normal user responses and then direct appropriate awareness programs to users accordingly

- Training Course Library with over 25 courses.
  Each course consists of series of short videos that the user can watch followed by comprehension questions to confirm that the knowledge has been understood.
  The training course library has courses which cover everything from the basics of understanding malware and phishing to more advanced topics such as Ransomware and Cybercrime.

- Reporting Center.
  Get phishing campaign statistics and generate per-user action reports and others to measure progress. The Campaign Executive Summary Report highlights the campaign data and results of the training so accountability and value is always clear.

### Implementation:

While there is no one size fits all user education program, however, the following is recommended:

- Running at least one to two phishing campaigns per month
- Running a minimum of one to three training courses per quarter
- Running compliance courses at time of need (usually driven by Audits)

An example of this would be:

| Month | Phishing Campaign | | Training courses |
|---|---|---|---|
| January | Microsoft 365 | Dropbox (Password Rest) | Data Security (Email) |
| February | Active Directory | Facebook Account Locked | |
| March | Adobe (Password reset) | | Data Security (Passwords) |
| April | Google security alerts | LinkedIn Invitation | Understanding Malware |
| May | Microsoft Account Reset | Microsoft 365 | |
| June | NetFlix Account reset | Paypal Payment Recieved | Data Protection |
| July | Facebook Account locked | | Introduction to Malware |
| August | LinkedIn Invitation | Active Directory | GDOR Express |
| September | Dropbox (Password Rest) | Google security alerts | |
| October | EFT Money transfer | | Understanding Cyber Security |
| November | Active Directory | NetFlix Account reset | Social Media Awareness |
| December | Microsoft Account Reset | | |

A complete overview of the Webroot Security Awareness Training can be found here:
https://www.webroot.com/us/en/business/security-awareness