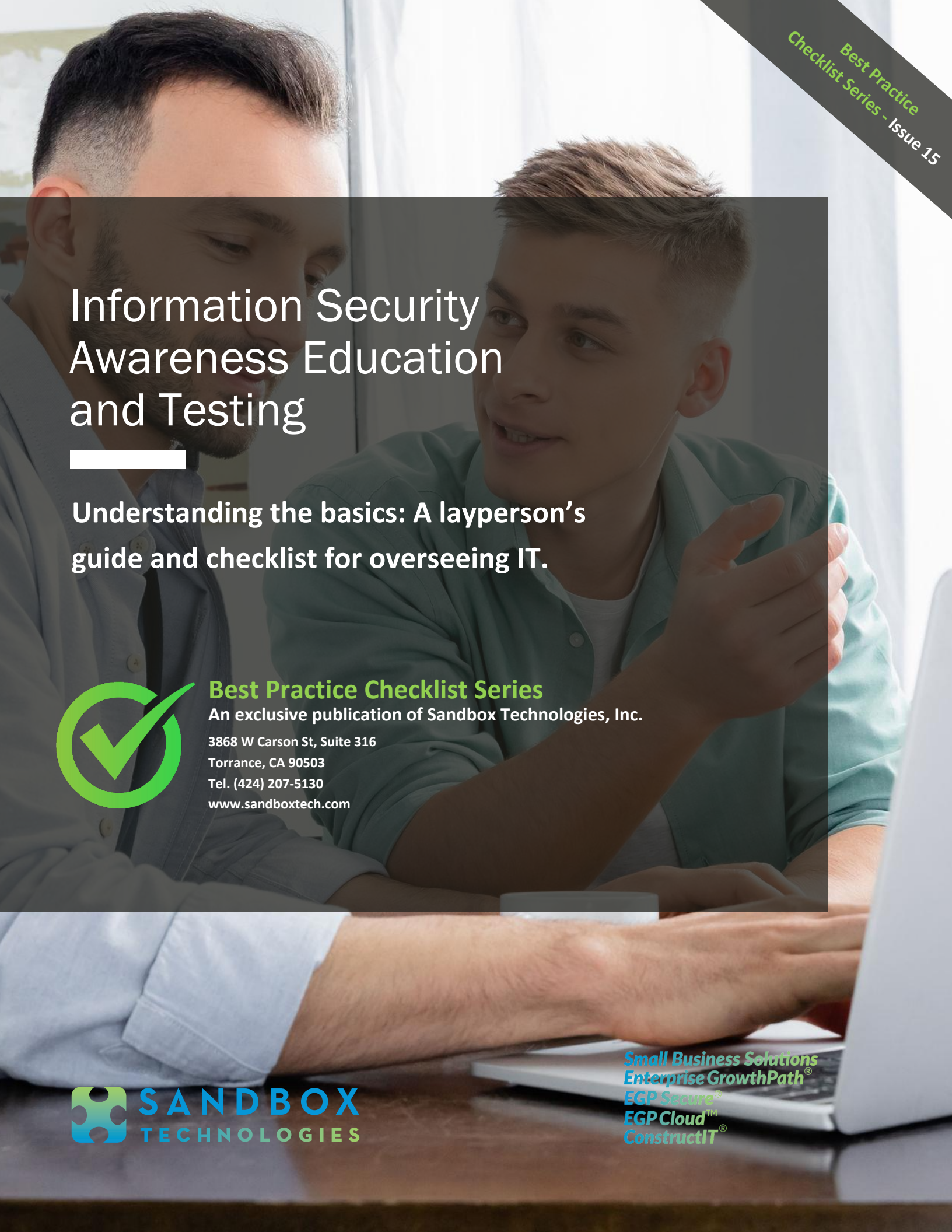


Best Practice Checklist Series - Issue 15

Information Security Awareness Education and Testing

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series

An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Information Security Awareness Education and Testing

Many network security failures are the direct result of phishing and other social engineering methods that target users.

Such dangers cannot be eliminated with technical measures alone. Recent data from the ITRC (Identity Theft Resource Center) cite phishing, ransomware/malware, and skimming as the primary vectors of attack in 63% of overall breaches reported. According to a report published by the Gartner Group,

"*The greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defences…*"

To successfully navigate today's threat landscape, technical protections are no longer enough. A savvy, well-educated user base is essential. In the pages that follow, a number of essential topics are addressed, and formal, recurring information security awareness training is recommended to help protect your organization's network against outside threats targeting users and other personnel.

For those interested, Sandbox Technologies offers all of the foregoing, as well as various phishing and other tests designed to help validate the adherence of staff members to the practices taught. As always, should you wish to discuss your current settings and protections, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Information Security Awareness Education and Testing 4

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Information Security Awareness Education and Testing

Understanding Threat Vectors

Do users understand that compromises can occur as a result of opening attachments, clicking on links, downloading images, and even responding to emails or providing information in any way?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Basic Habits

Are users routinely advised to "Stop & think", "Listen to their instincts", recognize signs of potential malicious activity, and "Inspect and verify" before taking actions, along with the importance of reporting any signs of malicious activity?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Phishing Tactics

Have users been taught how to recognize phishing tactics and avoid them?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Risk Destinations

Have users been educated regarding types of Web destinations that constitute risks and how to avoid them?

Examples include torrent/illegal file sharing sites, free online games & downloads, online pharmaceutical sales sites, pornographic sites, and some gambling websites.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Avoidance of Unrecognized Websites

Have users been taught the importance of avoiding websites that are unrecognized?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Matching Names

Have users been taught to confirm that the name of the URL being visited matches the actual name of the intended Web destination?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

HTTPS

Do users know to check for HTTPS:// preceding Web destinations to confirm protection by a valid security certificate?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Certificate Errors

Are users aware of the importance of NOT ignoring certificate errors?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Avoidance of Public Networks

Are users cautioned to avoid the use of public networks?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Company Owned and Approved Computers Only

Are users prohibited from accessing the company's network from any computer(s) or device(s) not owned and/or approved by the organization's IT and senior management?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

No Access to Cloud Services Except via Authorized Computers

Have users been explicitly prohibited from accessing company Cloud-based services using any computer(s) or devices(s) not owned and/or approved by the company's IT department and senior management?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Avoidance of Automatic Wi-Fi Connections

Does the organization prohibit users from connecting to Wi-Fi networks automatically?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Unnecessary Use of Company Email Addresses

Have users been advised that when creating insignificant or unimportant accounts online that they should avoid the use of company email addresses and addresses that identify them or the company in any way?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Social Media

Do users understand the importance of limiting personal information on social media accounts, not discussing company-related matters without authorizations, and restricting access to "friends" only when possible?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Passwords

Have users been prohibited from sharing their passwords with anyone else, including co-workers?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Unique Passwords

Does the organization counsel users to avoid utilizing passwords associated with company accounts (including their own) for access to other resources?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

On Premise Threats

Have users been taught how to identify and respond to various types of threats that involve direct, on-site contact and telephone contact?

Examples include requests to print a document from an individual's USB drive, requests for names of IT personnel, requests for equipment information or model numbers, and calls impersonating technical support organizations with questions, or "offering assistance".

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Removeable Media

Do users understand the importance of never inserting removeable media of any type, how to identify suspicious media, and the importance of alerting IT personnel immediately upon encountering any such media?

Means of deception can include labeling that piques curiosity (e.g., "Confidential", "Payroll", "Eyes Only", etc.), as well as the use of distinctive, familiar, or actual company branding and logos on devices left unattended, sent via mail or other courier, left in parking lots, or delivered to a receptionist or member of security.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Use of Designated Storage Locations Only

Are users apprised of the importance of only storing data on company authorized servers and/or company designated Cloud repositories?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Lock Workstations

Are users instructed to lock unattended workstations immediately?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Media Destruction

Are users instructed in the proper methods of destroying media when it is no longer required?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Avoidance of Password "Remembering" Features

Are users instructed to decline any and all offers to electronically store or "remember" passwords?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

No Literal Answers to Secret Questions

Have users been instructed to avoid the use of literal answers to "secret" questions (e.g., "What is your mother's maiden name?)

In an age where almost any information can be found online with enough effort, the notion that requiring an answer to many of the "secret" questions websites use to safeguard user credentials borderlines on insanity.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Avoidance of Incremental Password Changes

Have users been taught to avoid incrementally changing passwords by increasing a number or making an insignificant change when a password change is required?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Long and Complex Passwords Avoiding Dictionary Words

Have users been instructed to use lengthy passwords consisting of letters, numbers, and special characters while avoiding the use of individual or compilations of words that can be found in a dictionary?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Bad Password Idea Avoidance

Have users been taught how to avoid the use of common password selection practices that may seem original and difficult to guess, but in fact are not?

Examples include substitution of special characters for similar-looking letters (ex., "@" for "a", etc.), combining birth, graduation, or other dates with individual words (ex., "1968Mustang", "Quarterback88", etc.), using common phrases (ex. "AreWeHavingFunYet", "I Hate<Insert Political Figure>" "I Love<Insert Political Figure>", and using passwords containing any personal details that could be discovered with a bit of research (i.e., your spouse's name, your pet's name, your school, your favorite sports team, your parents' telephone number as a child, etc.). Although of the foregoing may seem original, people tend to think in very similar ways and as such, they are in fact not.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Equipment Control

Have users been advised that they should NEVER leave equipment unattended in vehicles or anywhere else unsafe?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Equipment Control

Are users prohibited from allowing anyone to use company equipment, including mobile devices?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Transmitting Passwords

Have users been prohibited from emailing passwords under any circumstances?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Personal Information Storage

Are users prohibited against storing any all forms of PII (Personally Identifiable Information) in Outlook contact databases, Excel spreadsheets and other non-approved repositories for sensitive information?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Cameras and Microphones

Have users been advised to obstruct cameras and disable microphones when they are not required?

Few are aware that compromised laptops, desktop computers and mobile devices are capable of recording audio and video unbeknownst to the user.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Scanning Protection

Have users been advised to maintain control of security access cards, and to securely protect mobile, Bluetooth and other devices that are susceptible to scanning?

Few people are aware of the risks that can stem from unlawful scanning of access devices. Some of the most common card solutions used to secure access to facilities, parking structures and so forth can be copied in as little as seven seconds using devices costing less than $50.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

COVID-19 Security Risks

Have users been apprised of the numerous new risks that have arisen as a result of the COVID-19 home worker accommodations and minimum protections that should be employed to help safeguard against them?

Although best practice recommendations call for the deployment of company owned and controlled computers for any and all access to company systems, for those organization where this is not possible, remote computers should, at a minimum, employ working, up-to-date antivirus protection, be patched and updated regularly, use only current and up-to-date software versions and operating systems, feature hard drive encryption and removeable media restrictions, employ a device-based firewall, have sharing disabled, and connect via hard-wired connections instead of Wi-Fi. On occasions when the latter is impossible, Wi-Fi passwords should be complex, difficult to guess, discrete and secure. Wireless equipment should be current and properly configured, employing at a MINIMUM, WPA2 PSK encryption technology. Optimally, remote users should employ the use of separate networks and Internet connections for all business-related activity.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Report Anomalies and Suspected Breaches

Last, but by no means least, have users been instructed to report any and all anomalies and suspected malware, trojans, breaches, etc. to the organization's management personnel and IT staff members IMMEDIATELY?

It is important to note that while mistakes are human and can be forgiven, failure to report them is vastly more egregious, and can cost an organization valuable time that could be used to curtail malicious actions and thwart breaches that might otherwise result in significantly more severe damage to the company.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2021, All Rights Reserved. Sandbox Technologies, Inc.