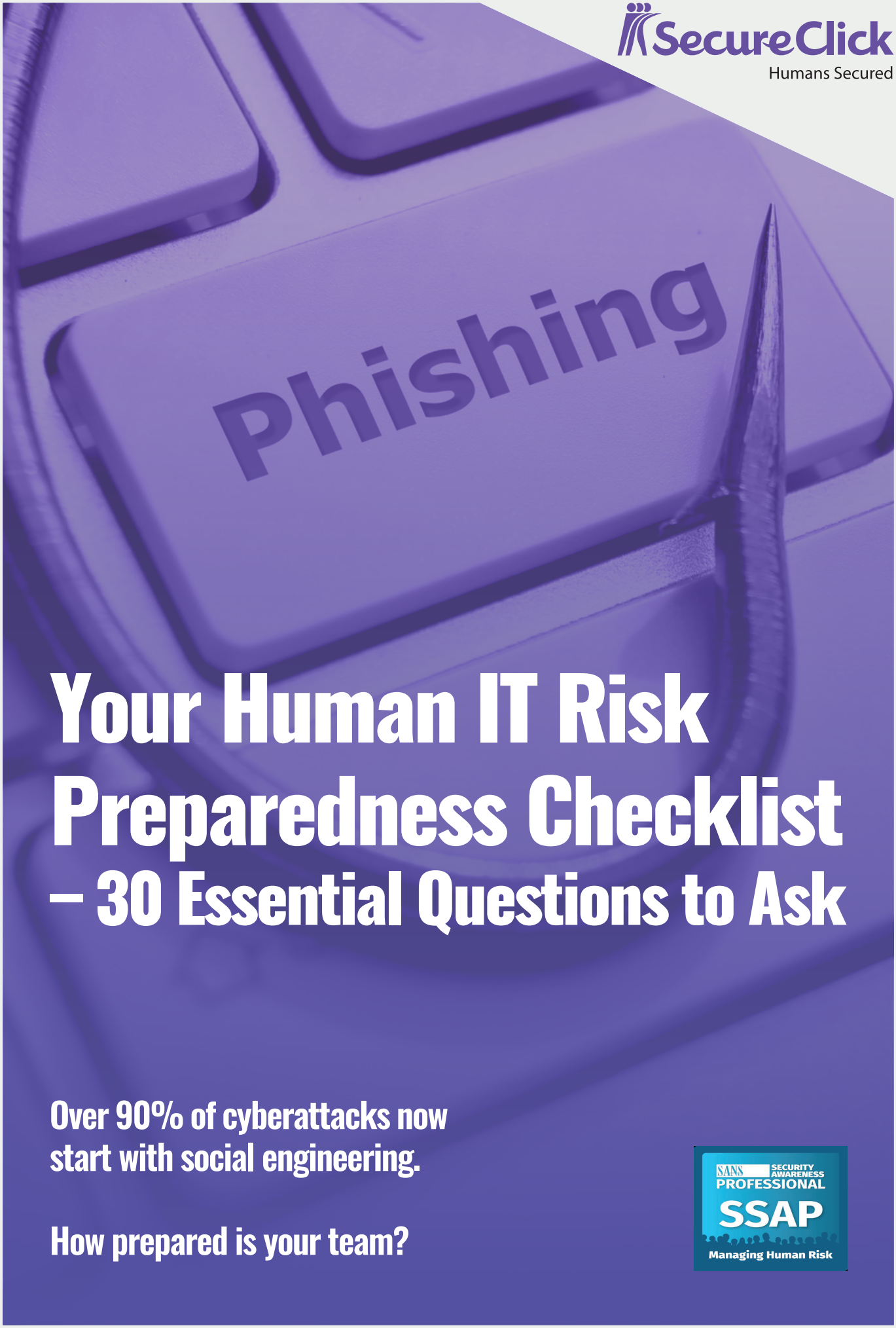
SecureClick
Humans Secured



Your Human IT Risk Preparedness Checklist – 30 Essential Questions to Ask

Over 90% of cyberattacks now start with social engineering.

How prepared is your team?

SANS SECURITY AWARENESS PROFESSIONAL SSAP Managing Human Risk

Every team member is different, but do you generally agree or disagree with the following statements?

Ramifications of a Cyber Attack or Data Breach

My team understands the operational, financial, and reputational ramifications of a cyberattack or data breach could have on our organisation. They understand that recovering from such incidents often involves much more than password changes and data restoration from backups.

Accountability

My team understands the inherent weaknesses of technical defences such as firewalls, email gateways, and end-point anti-virus. They understand that **humans are often the last line of defence.**

Technical Defences

My team understands that even devices that are in **"locked-down"** mode are still liable to malware attacks because of so-called "privilege escalation" techniques commonly used by cybercriminals. They understand that using a locked-down device does not preclude it from being compromised by malware.

My team understands that cybercriminals can often **bypass network firewalls, email gateways, and end-point anti-virus solutions**. They understand that technical defences are not a catch-all and vigilance still needs to be used when opening links, attachments, or downloading applications.

My team understands the importance of **two-factor authentication** in acting as a safety net against email account, VPN, and database compromise. They also understand how defences like two-factor authentication can be bypassed.

Cybercriminal Research

My team has a basic understanding of how cybercriminal groups **research them and their organisation** in order to launch more targeted attacks using very credible pretexts. My team also understands how **new employees** are at an enhanced risk level.

Credential Theft

My team understands the potential credential theft implications of using their work email address to register on non-work related websites.

("Credential theft" refers to the act of stealing someone's login credentials, such as usernames and passwords, to impersonate the victim and gain unauthorised access to their email accounts, VPN, or cloud storage service. Credential theft is a common precursor to ransomware.)

Email Phishing

My team understands that a cyberattack or data breach can start from inadvertently opening just one attachment or weblink contained in an email.

My team understands just how easy it is to **fake the email address** of a trusted entity such as a supplier, customer, or work colleague. (Email spoofing attacks can occur even if SPF, DKIM, and DMARC authentication is used.)

My team understands how almost **all email attachments can be potentially dangerous**.

My team understands how cybercriminals use dedicated Office 365 phishing kits to send credible-looking Microsoft-themed notifications and links to **very authentic appearing Office 365** portals that steal credentials.

My team understands that not all phishing attempts involve email attachments. They understand how cybercriminals exploit trusted cloud-based **collaboration services** like Dropbox and OneDrive to propagate malware.

My team understands the basics of how **email thread hijacking** attacks work. These occur when a historic email conversation thread with a trusted entity is suddenly "re-activated" to dupe the user into downloading data-stealing malware.

My team understands how **reverse or call-back phishing works**. This occurs when, for example, cybercriminals send a payment receipt to a user for a service which they never subscribed to. It is designed to shock the user into calling a bogus phone number (listed on the receipt), whereby they are then socially engineered to divulge passwords or inadvertently install malware onto their device.

My team understands the basic techniques which hackers use to **bypass two-factor authentication** controls.

My team understands how **multi-stage email phishing attacks** work, where a combination of telephone, SMS, QR code, or email messages are sent to trick them into revealing passwords, installing malware, or paying bogus invoices.

Impersonation

My team understands the basic mechanics of how **website cloning** of legitimate websites is used to steal passwords, or masquerade as trusted suppliers or other trusted entities such as government agencies or banks. My team also understands how their **IT support or security teams** can be impersonated to steal passwords, or used to persuade them into installing data-stealing malware.

My team understands just how easily the phone number or email address of their CEO or other colleagues can be spoofed to carry out invoice fraud or propagate malware.

Internet Browsing Behaviour

My team understands the dangers of inadvertently installing **malicious internet browser extensions** that can exfiltrate data (from Safari, Chrome, Firefox, etc.) to cybercriminals without being detected by firewalls or end-point security software.

My team understands how **Oauth phishing** works. This occurs when a seemingly innocent (but malicious) website asks a user to log in with their Office365 or Google Workspace credentials. While the ostensible purpose is to make logging in to a website easier, the real reason is credential theft.

SMS Phishing (Smishing)

My team can recognise **SMS phishing** attempts, even those that merge seamlessly into existing SMS conversation threads.

SEO Poisoning

My team can recognise **"SEO Poisoning"** attacks whereby malware-infected versions of popular software applications (such as VPNs) often appear in Google's search results, inadvertent installation of which can result in data exfiltration, credential theft, and ransomware attacks.

Malvertising

My team can recognise and understand the malware risks of seemingly innocuous clickable online advertisements.

Malspam

My team understands that emails masquerading as RFPs or marketing content can be infected with data-stealing malware, culminating in data breach incidents or ransomware attacks.

Psychological Triggers

My team can identify the common psychological triggers (such as curiosity) used by cybercriminals to persuade users to open email attachments and URLs (web addresses) and inadvertently divulge confidential information.

Device and Application Security

My team understands the databreach risks of using devices such as unencrypted laptops, or portable data storage media such as USB drives

My team understands the risks of using **outdated devices** and **applications**. They also understand the risks of **lending their work computing devices** to family members or housemates.

Secure Password Management

My team understands that **weak passwords, or password reuse** is still a leading cause of cyberattacks in 2024. They understand what constitutes a weak password and how some seemingly robust passwords can be cracked using so-called "wordlist" attacks.

Unintentional Data Exposure

My team understands the implications of unintentional data exposure. They also understand the most common ways data leaks can happen and how to prevent them.

Business Email Compromise

My team can detect the tell-tale signs of a business email compromise attack. They're also conversant with some of the techniques cybercriminals use to circumvent the processes which organisations have put in place to prevent BEC attacks.