WORLD COMPLIANCE ASSOCIATION



# Plantillas bajo mínimos y WiFi de playa: la mezcla perfecta que dispara los ciberataques a empresas en verano

## La vulnerabilidad de muchas empresas aumenta estos meses debido a la combinación de plantillas bajo mínimos y a una relajación general de las medidas preventivas

El periodo estival suele asociarse a la desconexión y al descanso vacacional, pero para los departamentos de tecnología representa una etapa de máxima alerta. Los expertos en ciberseguridad advierten que los ataques informáticos a empresas experimentan un incremento aproximado del 30% durante estos meses de calor. Esta tendencia responde a una estrategia deliberada de los ciberdelincuentes, quienes aprovechan que las organizaciones operan con personal reducido y protocolos de vigilancia menos estrictos. No bajar la guardia resulta fundamental para garantizar la continuidad del negocio tras el regreso de las vacaciones.

Y es que la ciberdelincuencia no descansa cuando el resto de la sociedad se toma un respiro necesario, intensificando sus campañas de intrusión. Por ello, el nivel de protección debe ser una prioridad estratégica dentro del cumplimiento corporativo de cualquier empresa. Mantener la vigilancia activa es la única forma de evitar que un descanso merecido se transforme en una crisis reputacional. La vulnerabilidad de las compañías aumenta sobre todo debido a la combinación de plantillas bajo mínimos y una relajación general de las medidas preventivas. Durante el verano, muchos empleados trabajan de forma remota desde ubicaciones poco habituales, lo que multiplica los vectores de entrada para posibles intrusiones. Los atacantes son plenamente conscientes de que el departamento de informática puede estar vacío o con menos recursos técnicos disponibles.

Esta situación crea un entorno perfecto para que los intentos maliciosos tengan una mayor probabilidad de éxito que en otros meses del año. Es común que los protocolos de acceso se vuelvan más laxos para facilitar la operatividad de quienes cubren las ausencias. Además, la contratación de personal temporal para sustituciones añade un riesgo extra si no existe una formación de seguridad adecuada. Por tanto, la seguridad no debe verse como algo técnico, sino como un pilar organizacional fundamental. La concienciación debe ser el primer cortafuegos ante cualquier amenaza que busque explotar el factor humano.

Entre las amenazas más recurrentes en esta temporada, el phishing se posiciona como la técnica preferida debido a su alta efectividad. Se estima que los intentos de suplantación de identidad por correo electrónico aumentan significativamente, especialmente los dirigidos a individuos específicos. Los delincuentes utilizan ganchos relacionados con reservas de hoteles, billetes de avión y ofertas turísticas para engañar a los trabajadores desprevenidos. Además del fraude al consejero delegado y el robo de identidad, el ransomware sigue siendo una preocupación crítica para los expertos. Estos ataques buscan cifrar la información sensible de la empresa para exigir un rescate económico por su posterior liberación. La sofisticación de estos mensajes maliciosos hace que incluso el personal más experimentado pueda caer en la trampa.

Para mitigar estos riesgos, implementar la autenticación multifactor en todas las cuentas corporativas se considera una medida de primer orden. Este sistema añade una capa de verificación adicional que dificulta enormemente el acceso no autorizado a los recursos críticos. Asimismo, es imperativo realizar una actualización exhaustiva de todos los sistemas y software antes de iniciar el periodo de vacaciones. Los parches de seguridad corrigen vulnerabilidades conocidas que los hackers intentarán explotar si no están debidamente cerradas. La automatización de las copias de seguridad es otro pilar fundamental para asegurar la recuperación de datos ante un desastre.

El uso de conexiones remotas seguras es indispensable para aquellos trabajadores que mantienen su actividad laboral durante el periodo estival. Desde el Instituto Nacional de Ciberseguridad recuerdan que “durante las vacaciones de verano se visitan aeropuertos, hoteles, etc. En casi todos estos lugares existe la posibilidad de conectarse a Internet a través de redes Wi-Fi públicas. Como no sabemos quién las gestiona, ni quién puede estar conectado, es preferible no conectarse a ellas. Antes de acceder a servicios online con usuario y contraseña, asegurarse de que la dirección empieza por ”https“, y mucho mejor emplear una ”VPN“.

Además, se debe ejercer un control estricto sobre los dispositivos móviles que se utilizan para fines laborales. Implementar políticas de cifrado, contraseñas robustas y la capacidad de borrado remoto es vital en caso de pérdida o robo. Limitar los accesos al personal estrictamente autorizado reduce significativamente el radio de impacto de una posible brecha. El principio de mínimo privilegio asegura que cada usuario solo acceda a lo que realmente necesita.

“La seguridad depende, sobre todo, de las personas”, afirma Jordi Alarcón, responsable de IT de Esofitec, empresa especializada en soluciones tecnológicas de facturación, contabilidad, gestión y recursos humanos: “Nos relajamos, asumimos la carga de compañeros de vacaciones o seguimos revisando el correo corporativo desde el móvil, sin estar tan alerta, lo que facilita que acabemos haciendo clic en enlaces maliciosos. Por eso, si vas a teletrabajar desde un entorno no habitual, evita conectarte a wifis abiertas y mantén el Bluetooth o el AirDrop desactivados. Y, si eres responsable de ciberseguridad, aprovecha para revisar el protocolo de copias de seguridad y activar protocolos de ciberresiliencia.”

## Cómo reaccionar

La formación del personal, incluyendo a los sustitutos temporales, constituye una de las mejores inversiones en materia de seguridad informática. Es crucial que los nuevos empleados conozcan los protocolos de la empresa y sepan identificar los ataques más comunes. No descargar aplicaciones de origen dudoso ni archivos adjuntos sospechosos son pautas básicas que deben reforzarse constantemente. La curiosidad por ofertas vacacionales o guías de viaje en formato PDF puede esconder virus informáticos altamente peligrosos. Además, se recomienda moderar la información que los empleados publican en sus perfiles personales de redes sociales. Compartir la ubicación en tiempo real o las fechas exactas del viaje puede dar pistas valiosas a los atacantes.

Contar con un plan de respuesta ante incidentes bien definido permite actuar con rapidez si ocurre una intrusión accidental. Todos los miembros de la organización deben saber a quién contactar y qué pasos iniciales seguir de forma inmediata. La detección temprana de comportamientos anómalos en los equipos puede evitar un desastre de mayor impacto reputacional. Antes de cerrar por vacaciones, realizar una búsqueda proactiva de brechas de seguridad ayuda a blindar el entorno digital. Por eso, en verano la ciberseguridad sigue siendo una necesidad imperativa para la supervivencia empresarial. Proteger la infraestructura tecnológica significa salvaguardar la confianza de los clientes y la reputación de la marca. Los ciberdelincuentes no se toman vacaciones y su actividad se intensifica precisamente cuando detectan una menor vigilancia.

Fuente: Plantillas bajo mínimos y WiFi de playa: la mezcla perfecta que dispara los ciberataques a empresas en verano