May 2024

modernnetworks

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

91% of successful cyber-attacks start with an email

On average, a person receives 121 emails related to business every day. Like it or loath it, email remains a critical communication channel for businesses. However, its very popularity makes email a prime target for cybercriminals seeking to exploit vulnerabilities and compromise sensitive data. As an IT managed services provider, we understand the paramount importance of securing your organisation's email communications.

Why Email Security Matters:

- **Phishing Threats:** Phishing emails account for a staggering 91% of successful cyberattacks. These deceptive messages can lead to data breaches, financial losses, and reputational damage.
- **Malware and Attachments:** Viruses often infiltrate systems via seemingly innocuous email attachments. Our robust email security measures include real-time scanning to identify and block harmful links and attachments before they reach your inbox.
- **Social Engineering Attacks:** Cybercriminals are increasingly sophisticated, using social engineering techniques and the latest AI technologies to impersonate trusted contacts and extract sensitive information. Our solutions help to guard against these advanced attacks.

How We Can Help:

- **Customised Solutions:** We can tailor email security solutions to your specific business needs. Whether it's spam filtering, encryption, or data loss prevention, we've got you covered.
- **Ongoing Support and Management:** Our team ensures that your security options remain up-to-date and effective against evolving threats. We're here to support you 24/7.
- **Education and Awareness:** Security awareness is key. We educate our clients about risks, including phishing and social engineering, empowering your team to stay vigilant.

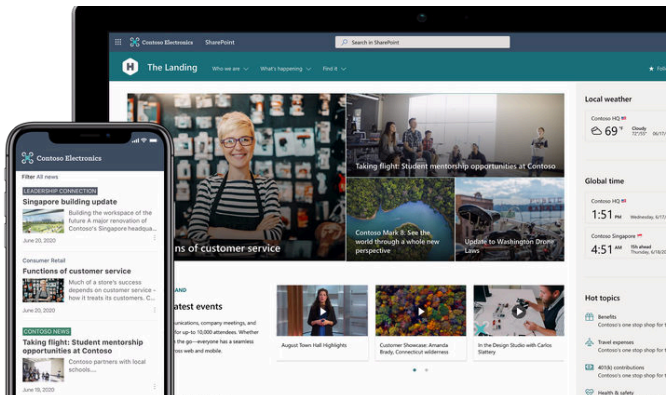
Claim Your Free Guide

We're excited to offer you a complimentary guide that examines the importance of email security and provides actionable best practices. Learn how to safeguard your organisation against threats, enhance employee awareness, and fortify your email defences.

DOWNLOAD NOW

IN THIS EDITION

Seven New Features in Microsoft SharePoint



SharePoint and OneDrive in Microsoft 365 are Cloud-based services that help organisations share and manage content, knowledge, and applications to empower teamwork, find information quickly, and facilitate collaboration.

SharePoint is constantly evolving and improving. Here are seven of the latest features and benefits:

1. **Copilot in SharePoint:** Introduced on May 2, 2023, the Copilot AI assistant can help you transform existing content into stunning SharePoint pages. It's a great tool for creating engaging and visually appealing sites.
2. **Design Video with Microsoft Stream:** You can now incorporate videos throughout SharePoint using Microsoft Stream. This feature allows you to enhance your SharePoint pages with multimedia content.
3. **Refreshed OneDrive Experience:** OneDrive has been revamped to be faster, more organised, and personalised. If you use OneDrive alongside SharePoint, you'll appreciate the seamless integration between the two.
4. **Modern Site Pages and Web Parts:** SharePoint now offers modern site pages and web parts, making it easier to create dynamic and responsive content. These modern components enhance the user experience and allow for greater customisation.
5. **Integration with PowerApps, Power BI, and MS Flow:** SharePoint integrates seamlessly with other Microsoft tools like PowerApps, Power BI, and MS Flow. This integration enables you to build powerful workflows, automate processes, and visualise data within your SharePoint environment.
6. **Improved Search Capabilities:** SharePoint's search functionality has been enhanced, making it easier to find relevant content across your sites and libraries. The improved search experience helps users quickly locate the information they need.
7. **SharePoint Home Page:** The SharePoint home page provides a centralised hub for accessing sites, news, and recent activity. It's a convenient starting point for users to navigate their SharePoint environment.

Remember that SharePoint is continually evolving, so staying up-to-date with the latest changes is essential.

Useful links:
You can find more information on the official Microsoft Support page and explore additional resources there.
Learn more about the new era of SharePoint and OneDrive in Microsoft 365.

Protecting Commercial Property: The Critical Role of Cyber Insurance

Research by the insurer Aviva found that businesses are 67% more likely to experience a cyber-attack than a burglary or building fire. In today's uncertain world, cyber insurance can help safeguard the operators of commercial buildings against the financial consequences of cyber incidents. In this article, we discuss the increasing importance of IT systems in the management of commercial buildings and cyber insurance as a component of a comprehensive cyber resilience strategy.

The Importance of Cyber Security for Commercial Property

In scenarios where an office complex or retail centre lacks comprehensive cybersecurity protection, they jeopardize not only their data integrity and operational functionality but also their eligibility for insurance coverage. Insurance providers are increasingly instituting rigorous cybersecurity criteria as a necessary condition for offering coverage. Non-compliance with these conditions may result in the denial of insurance coverage or the termination of existing policies, consequently exposing property owners and operators to significant financial risks.

Hackers Take Control of Building Automation Systems

In 2021, a sophisticated cyber-attack on a German building engineering firm caused significant disruptions by seizing control of hundreds of Building Automation System (BAS) devices that managed functions like light switches, motion detectors, and shutter controllers. The attackers exploited digital security keys to lock out the company from its own systems, leading to a loss of smart functionalities across numerous devices. Security experts were able to recover the compromised system by extracting the hijacked key from a damaged device, underscoring the urgent need for enhanced cybersecurity measures in the management of interconnected building systems. A year later, Security Week published a story about a vulnerability in Siemens Building Automation Controllers that could render them unavailable for days if successfully attacked.

NEXT

Managing Risk

In response to a continually evolving range of cyber threats, the cyber insurance market has matured, with insurers now requiring evidence of proactive cybersecurity measures before offering coverage. This shift reflects a broader recognition of the integral role that cyber insurance plays in the risk management strategy of many businesses including commercial real estate. By transferring some of the financial risks associated with cyber incidents to insurers, businesses can better manage the aftermath of an attack, including legal and regulatory actions, and focus on restoring operations and reputation.

The Threat Landscape

Commercial building owners and operators face increasing cyber threats. Phishing, social engineering, ransomware, malware, and data breaches are all common. Cybersecurity weaknesses in commercial real estate include Wi-Fi networks, wireless peripherals, key card access, HVAC systems, power supply hardware, and portfolio management software. Smart building technologies such as IoT devices expand the attack surface for potential cyberattacks. Insider threats from malicious staff and human error also present significant risks, as do complex supply chains and third-party service providers.

$8 Million Per Day Failure

In 2018, a Las Vegas casino fell victim to hackers through a smart thermometer. The casino had installed this thermometer to monitor the water temperature of an aquarium in its lobby. However, cybercriminals exploited a vulnerability in the thermometer to gain a foothold in the casino's network. Once inside the network, they targeted the high-roller database, extracting sensitive information about the casino's biggest spenders and other private details. Similarly, MGM Resorts International experienced a significant cyber-attack that led to a 10-day computer shutdown including hotel reservations and credit card processing. While specific details about the extent of the breach have not been disclosed, experts estimate that the shutdown cost MGM Resorts up to $8 million per day. These incidents serve as a stark reminder that the proliferation of IoT devices makes organisations and infrastructure more vulnerable to cyber-attacks.

Cyber Essentials

The evolving nature of cyber threats means that yesterday's security measures may no longer suffice. The National Cyber Security Centre (NCSC) advises organisations to adopt recognised cybersecurity defences, such as those certified by Cyber Essentials or Cyber Essentials Plus, to enhance their security posture and potentially qualify for insurance discounts.

NEXT

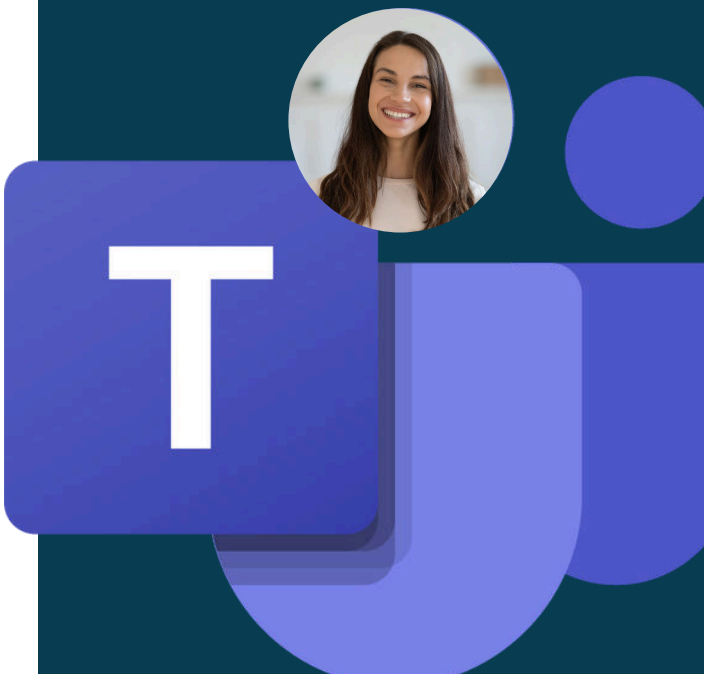
NEW TO

MICROSOFT

Check a User's Presence and Availability in Teams

In the new Teams, you can simply click on a user's avatar or profile photo to quickly get an overview of their online status, the next available calendar slot in Outlook, work hours, local time, or work location (remote or in-office).

The Follow User's Presence and Availability feature in Microsoft Teams allows you to efficiently communicate, schedule meetings, and collaborate by tracking the online status and availability of your colleagues.



5 Criteria for Cyber Insurance:

1: Security awareness training educates employees with the knowledge and skills to protect an organisation's data from hacking, phishing, and other breaches. Additionally, testing involves assessing employees' ability to identify and counter cyber threats, often through real-world phishing scenarios, reinforcing security awareness and behaviour change.

2: Multi-Factor Authentication (MFA) enhances security by requiring multiple credentials (such as a password and a code from an authentication app) to access IT systems and resources, making it more robust than traditional username-password combinations.

3: Endpoint Detection and Response (EDR) is a security approach that concentrates on the endpoint environment, including devices such as laptops and desktop computers. The goal is to collect data that can be used to quickly detect, contain, and remedy any security threats. In contrast, Managed Detection and Response (MDR) provides a more comprehensive view of the network by analysing data from various sources. This allows for real-time detection and response to any potential security threats.

4: Data backup best practice is known as the "3-2-1" rule. The rule requires an organisation to maintain three copies of backup data, stored across two different mediums, with one copy stored securely off-site such as the Cloud.

5: Vulnerability management is a continuous and regular process of identifying, assessing, reporting, managing, and fixing cyber vulnerabilities present across IT systems. Security teams use various vulnerability management tools to detect vulnerabilities and implement different processes to patch or remediate them.

Commercial building owners and operators will face difficulties in obtaining cyber insurance coverage without adequate security controls. Furthermore, it's essential to keep in mind that security is an ever-evolving concept. While many insurers currently require five core security elements to consider a firm's eligibility for coverage, the requirements might change by the time you renew your policy. Therefore, it's vital to stay up to date with security matters.

Help Meet Cyber Insurance Criteria

As an IT Managed Services Provider (MSP), **Modern Networks** helps property companies obtain or renew cyber insurance coverage. We do this by ensuring that your company's IT infrastructure aligns with the required security standards and best practices. We help identify vulnerabilities, implement robust security measures, and provide evidence of compliance to insurers. Additionally, our team can work with you to assess risks, evaluate policy options, and facilitate the application process, ultimately safeguarding your organisation against cyber threats and potential financial losses.

Today, the commercial real estate sector needs to prioritise cybersecurity as it embraces new technologies. Cyber insurance is more than just a financial safeguard; it's a key element of a robust cybersecurity plan. With cyber threats evolving, the industry needs to update its security strategies. Cyber insurance is crucial in reducing these risks and keeping businesses running smoothly. Commercial property companies need to meet the cybersecurity standards set by insurers to protect their assets, reputation, and financial health. Partnering with Modern Networks gives our customers the necessary IT support and expertise to defend against cyber threats, meet the strict cyber insurance criteria, and retain the trust of stakeholders.

To learn more about how **Modern Networks** can help landlords and managing agents of commercial buildings remain cyber-secure and insurance-compliant, contact us today. You can call us on **01462 426500.** Alternatively, **visit our website.**

Visit The National Cyber Security Centre (NCSC) website for cyber insurance guidance.

Q: Does the current tech solution support what my business does best?

As a small business, it's essential to choose technology that aligns with your core competencies and business operations. Regularly assess whether your existing tech solutions still meet your needs or if they need updating. Adaptability and scalability are key factors to consider.

Q: Am I comfortable with the level of risk?

Every technology choice involves some level of risk. Evaluate the potential risks associated with adopting a particular solution. Consider factors like security vulnerabilities, compatibility issues, and the impact on your business operations. Make informed decisions based on your risk tolerance.

Q: Do I have what it takes to surpass customer expectations in a digital world?

Technology plays a significant role in meeting customer expectations. Consider how your business can leverage technology to enhance customer experiences. Whether it's through a user-friendly website, efficient communication channels, or personalized services, prioritize meeting customer needs.

modernnetworks

To get in touch with us:
Call 01462 426500
Email info@modern-networks.co.uk
Web www.modern-networks.co.uk