Identifying a data breach

Essential checklist

Signs of a data breach	What to look out for
Unusual network activity	Anomalies on your network activities and suspicious behaviour like increase in network traffic, unusual data transfers or unauthorized access attempts.
System slowdowns	Unexpected and unexplained slowdowns or performance issues on your network and system.
Unauthorized access	Login attempts from unfamiliar locations or unusual login times trying to access sensitive data, systems or accounts.
Changes in system settings	Unauthorized changes to system settings, configurations or user permissions that are not part of routine maintenance.
Unexplained data loss	Unusual changes to data or backups such as unexplained modification, deletion, or encryption.
Phishing emails	An increase in phishing emails targeting employees can indicate an attempt to gain unauthorized access.
Security warnings	Security alerts from your cybersecurity tools, antivirus software or intrusion detection systems.
Uncommon account activity	User accounts with unusual activity, such as changes in user permissions or suspicious transactions.
Unexpected pop-ups or messages	Pop-ups, error messages or warnings that appear unexpectedly on your system.
Customer reports of suspicious activity	Customer complaints about unauthorized charges, account compromises or suspicious activities.

It can be demanding to manage a business and be attentive to the signs of a data breach, which is why having a trusted managed IT partner can help improve your chances of detecting and mitigating breaches before they can cause more damage to your business. TELUS Business can help you implement a layered approach to cybersecurity to help prevent cyberattacks.

Connect with a managed IT specialist today to learn how we can help with your cybersecurity needs.

telus.com/FullyManaged

TELUS Business