

Are you protected from phishing and ransomware, the two most common threat scenarios? Chances are, you may need some help.

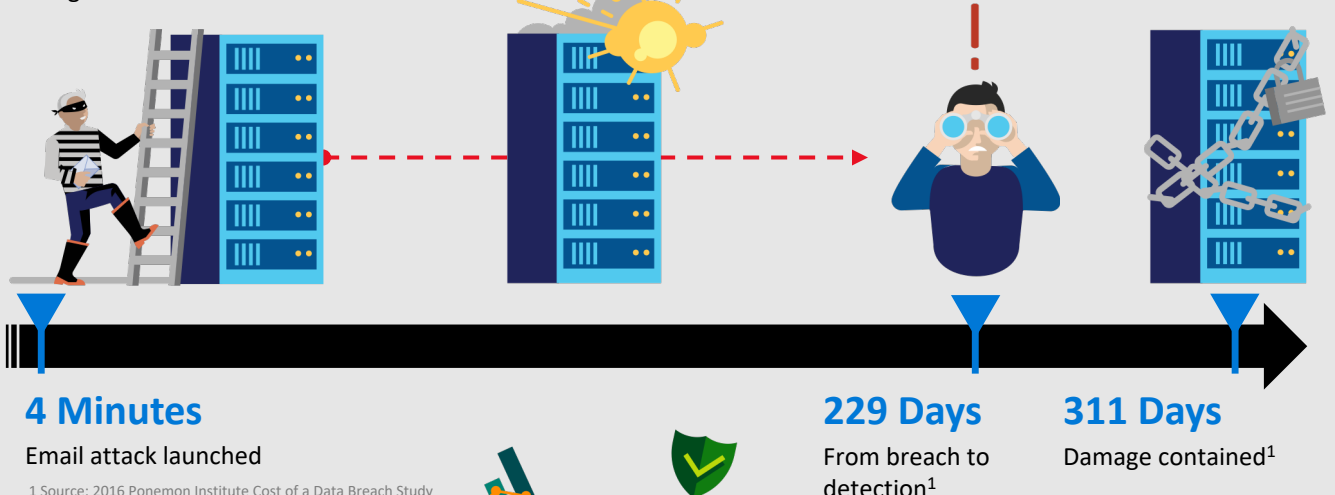
An illustration on a blue background showing a thief on the left and a man on the right. The thief, wearing a black mask, a black and white striped shirt, blue pants, and black boots with orange soles, is holding a fishing rod. The fishing line extends from the thief's rod, loops over the top of the man's laptop, and ends in a small blue bucket. The man, wearing glasses, a blue long-sleeved shirt, and red pants, is sitting in a white office chair at a grey desk, working on a silver laptop. A white envelope is on the desk next to the laptop. The scene is a metaphor for data theft.

75%

of individuals use only 3 or 4 passwords across all of their accounts.

*Source: Security Week Survey (ref. P35 of Security Playbook)

It can take over 7 months to discover a breach and another 80+ days to contain it. Plenty of time to inflict significant damage.



Do you know who is accessing your data?

Can you protect your data on devices, in the cloud, and in transit?

Can you grant access to your data based on risk in real time?

Can you quickly find and react to a breach?

The diagram illustrates the four pillars of Microsoft Security, each represented by a blue circle with a white icon and a corresponding text box below it. The icons are: a person with glasses and a red key for Identity & Access Management; a blue shield with a white padlock for Threat Protection; a white envelope with a blue padlock for Information Protection; and a blue toolbox with a white key for Security Management.

Identity & Access Management	Threat Protection	Information Protection	Security Management
Protect users' identities and control access to resources	Protect against threats and recover quickly when attacked	Confirm documents and emails are seen only by authorized people	Gain visibility and control over security tools

<https://www.microsoft.com/security>

Office 365 ATP
Protects your email, files, and Office 365 apps against attack vectors.

>99.9%
Malware catch rate

45 Seconds
Average file detonation time

Azure ATP
Helps protect hybrid enterprise environments from advanced targeted cyber attacks and insider threats.

Windows Defender ATP
Provides preventative protection, detects attacks and zero-day exploits, and gives you centralized management for your end-to-end security lifecycle.

The infographic is divided into three horizontal sections. The top section features a yellow sun icon with rays and a document icon with a magnifying glass. The middle section features a green virus icon. The bottom section features a blue shield icon. The text is arranged in a clean, modern font, with key metrics highlighted in large, bold numbers.

The diagram is divided into three vertical sections, each with an illustration and a text block. The first section, 'Education and Assessment', features an illustration of a man pointing at a chalkboard with diagrams of a padlock, a lightbulb, and a bar chart, while a woman sits at a laptop. The second section, 'Proof of Concept', shows an illustration of a rocket launching from a blue base with a rocket icon on it. The third section, 'Ongoing Security Services', depicts a woman holding a smartphone, surrounded by icons for a bar chart, a padlock, a speech bubble, and a download arrow, all connected by a network of lines.

Education and Assessment

We can evaluate your security position, identify gaps, and create a roadmap to increased protection and security.

Proof of Concept

Understand how the security features in Microsoft 365 can be used within your specific environment and prioritize the implementation of key features based on your needs.

Ongoing Security Services

Need ongoing security support? No problem! We've got you covered to help you maintain and reinforce security and protection.