

USA: The New Security Reality

Google & YouGov | January 2022



In recent years there has been a significant increase in cyber attacks across the globe.

This has impacted many parts of life, but the increased threat has been especially real for high-risk users, those in the public eye such as journalists and politicians.

Google has worked with YouGov to understand how those working in these professions feel about the cyber threats posed to them, how these threats have evolved, and what they are doing to protect themselves.



High profile individuals in the USA are **feeling the strain** when it comes to cybersecurity

59% believe that their professions make them more likely to be a target of hacking or phishing

83% believe that the threat of cyber attacks on journalists and politicians has increased in the last two years

73% believe this is a result of increasingly sophisticated hacking/phishing techniques

And they have felt these threats personally. A large number have experienced a hack or have had content accessed without permission



41% have had digital accounts hacked or accessed by others without permission in the last 12 months alone

Politicos are more likely to have been hacked than journalists (82% vs. 52%)

The majority of high profile individuals in the US **demand greater cybersecurity protection**



85%

agree that cybersecurity protections for people in high profile roles need to be improved

Not one respondent disagreed with this view

This call for greater protection is likely due to **the complexity it adds to high profile roles**



51%

believe that increased threats have made their jobs harder to do

When it comes to **who holds most responsibility for device protection**, high profile individuals are divided

60%

politicos feel it's predominantly their IT Managers' responsibility

VS

79%

journalists feel it's predominantly their responsibility

Most politicos feel it's predominantly up to IT managers to ensure devices and data are protected, whereas most journalists feel they hold most responsibility themselves

Both groups choose to protect themselves in similar ways, with **passwords remaining a core focus**

POLITICOS' PREFERRED METHODS

44%

Two-factor authentication or security keys

44%

Using unique passwords for different accounts or devices

JOURNALISTS' PREFERRED METHODS

59%

Using unique passwords for different accounts or devices

54%

Two-factor authentication or security keys

Some techniques remain largely **unexplored**, despite the benefit and protection they could provide



Less than one in five (18%)

politicos are **only** using devices issued by their workplace



Only 4%

of journalists are increasing the amount they reference their organisation's security



Defend against targeted online attacks with Google's strongest account security

For most, Google's built-in account security is all they need to keep their information secure. But for people at risk of targeted attacks, we offer the [Advanced Protection Programme](#).

To date we have seen no evidence of a successful phishing attempt on accounts enrolled in the Advanced Protection Programme.

