Examining the Born Before Computer (BBC): Digital Vulnerabilities, Scams, and GRC Safeguards

By: Dr. Nuru-Deen Mohammed, CISM

Contributing Faculty,

Walden University

NuruDeen.mohammed@mail.waldenu.edu

Abstract

With so much of our lives in the digital world, an awareness of online risks is essential. This is true for both our private data and finances and those of employers. However, while younger generations have grown up with the internet are fully aware of the scams and security threats that we are all subjected to, those who grew up before the internet face unique challenges.

Known as Born Before Computers, or BBCs, as private individuals and especially as employees, they are more susceptible to digital fraud and represent risk to business integrity. As a result, it is important to adopt tailored Governance, Risk and Compliance strategies to help minimize those risks and protect BBC employees. This includes dedicated leadership, training and oversight, along with a range of strategies for equipment and more to minimize risk exposure.

Keywords

Born Before Computers; Digital Vulnerabilities; Cyberscurity Risks for older employees; GRC Safeguards for BBCs.

Introduction

For the generations that have grown up online, knowing the dangers of scams, hacking, and data theft has become second nature. So much so that understanding how to spot such scams is taken for granted. However, not everyone grew up online, and for the Born Before Computers (BBC) generation, things are a little different.

The BBC generation refers to those who were adults before computers and the internet became part of daily life. It may be a surprise to many, but around 19% of the US workforce is aged 65 or older (Fry & Braga, 2023), and the majority of these fall into the BBC generation.

That limited exposure to modern technology and the connected world has left them vulnerable to digital scams, and that can have significant consequences for individuals and employers alike. This article examines the vulnerabilities to scams that the BBC generation faces, how organizations can protect them, and the role of Governance, Risk, and Compliance (GRC) strategies in safeguarding sensitive data and financial assets.

Why the BBC Generation Falls Victim to Scams

To find ways to protect this generation, we must first understand the risk itself, and that means knowing how they fall victim to these scams in the first place, and which scams are most effective.

Psychological and Behavioral Factors

The BBC generation provides a unique combination of behavioral consistencies and psychological responses that make them especially vulnerable to online scams of all kinds (Grilli, et al., 2021). One of those is a deference to authority, which stems from the more traditional environment they grew up in (Holt, 2024). They were taught from an early age that those in authority were to be respected and obeyed unquestioningly, whether that was teachers at school or leaders at work. This is very different from modern thinking, where questioning authority is seen as normal.

That need to defer to authority often plays a role in scams, as it can lead to a lack of critical thinking, just following instructions if they are believed to come from a place of authority. This is combined with a basic lack of understanding of what digital fraud looks like, making it very difficult to spot the problem in advance. While most people who have grown up with the internet know what common frauds and scams look like, and can spot a dodgy link in a text message a mile off, the BBC generation doesn't have that innate understanding, so they struggle to see scams for what they are.

In addition, this group is particularly vulnerable to fear of loss, where very real 'buy before it's gone' offers meant that you could miss out by not getting involved. Scams that prey on rarity, or create a sense of urgency to act before it's too late, result in little research and a rush to get things done rather than thinking about consequences.

Common Types of Scams Targeting BBCs

These particular weaknesses make BBCs vulnerable to scams of all types, but there is a particular risk with the following (Morrison, Coventry, & Briggs, 2021):

- **Dating Scams** – Scams that feature emotional manipulation, such as preying on loneliness or faking romance, often find success with BBCs.
- **Phishing Scams** – The reverence for authority is leveraged in email and SMS scams that impersonate banks or employers.
- **Tech Support Scams** – Whether calls about computer problems or fake pop-ups, scams that focus on a lack of technical knowledge are often very effective with BBCs.

Strategies to Protect Individuals

Understanding the vulnerabilities of the BBC generation and how that is exploited by criminals helps us to develop strategies that protect these individuals. Obviously, this is important in private lives, but even more so in the workplace, where falling for a scam could place an entire network or database at risk of theft or attack.

Personal Digital Hygiene Practices

Protection begins at the device level, ensuring that each device has as much in-built protection as possible without leaving known vulnerabilities. This includes:

- **Regular Updates** – Ensuring devices are running the latest software and firmware reduces the risk of exploits.

- **Antivirus Software** – An essential tool for BBCs, especially products with real-time analysis, as it can spot viruses and other threats before the user activates them.
- **Password management** – Making use of a password manager to generate and store passwords is good practice. As an alternative, ensure that each user is aware that they must never share passwords, bank details, or other sensitive information via email or over the phone.

With the device itself and an antivirus package actively helping each user to avoid phishing scams and others, maintaining effective digital hygiene can go a long way to reducing overall risk.

Cybersecurity Education Initiatives

However, passive protection from digital hygiene practices can only do so much, and ultimately, the individual user has to take some responsibility. Given the issue for BBCs is that they simply did not grow up in a world where online threats were a thing, the most effective approach to this is via education.

By teaching them to understand what the risks look like, where they come from, and how to deal with them, BBCs can have the tools they need to safely operate in the digital world. Numerous approaches can be taken here, and these include:

- **Community-Based Training** – Combining discussions, games, and presentations to help groups understand the risks they are exposed to regularly.
- **Role Playing Workshops** – Focusing on the social engineering aspects of scams and threats, these workshops show each individual how they can be steered towards specific actions through behaviors they take for granted.
- **Cyber Guardians** – Using younger, tech-savvy mentors to help BBC users gain a better understanding of the risks and threats involved, along with appropriate responses.

The key to all these initiatives is to both provide information but also build confidence in each individual. Being the victim of a scam can have a long-lasting impact on confidence and self-worth (McDermott, 2012), so for individuals who are in training after an incident, it is important to deliver the right message. It is always a problem about criminal behavior, and the victim is never at fault.

The Employer's Role: Protecting the BBC Workforce

It is crucial that individuals do take responsibility for the risks they face in terms of scams and online threats, and that they have the tools to both identify and avoid them. However, it is also true that in the workplace, employers must not only take responsibility for the risks to their data, but they must also seek to minimize such risks.

BBC employees represent a risk to the data and digital infrastructure they have access to, whether via a company-owned device or their own. The job for employers is to minimize that risk, and there are several ways in which that can be achieved. The focus should always be on prevention, so limiting exposure, education, and risk management are at the heart of this process.

With the right support in place, BBC employees and the digital infrastructure of the business can be protected from cyberthreats of all kinds.

Preventing Business Data Leaks

Data is the most valuable asset any business owns, and protecting it should always be a core mission for any security initiative. This is a multi-faceted program that covers both process, policy, and training initiatives.

Access Control

If fewer people have access to critical data, there is less risk that the data may be compromised. Using an access control solution to restrict and monitor data access is an essential tool in maintaining oversight and minimizing risk.

Role-based permissions allow access to data as required, avoiding delays while obtaining access, maintaining smooth operations while allowing for early warning should any unauthorized access occur. There are a number of approaches to achieve this, with dedicated software solutions for security, although some data platforms, such as Microsoft Dataverse, include Role-based security as part of the system (Microsoft, 2025).

This approach has the advantage of not requiring any user training or oversight; once permission levels are set, nothing else is required. With role-based permissions, especially, users are allocated appropriate access automatically, requiring no further input.

Training

As with any sort of response to BBC risks, training individuals to identify scams and threats is crucial. Making sure employees can recognize phishing scams is especially important in the work environment, as with modern work practices, one vulnerability could leave an entire network at risk.

Specialized training provision for BBCs gives them the understanding they need to highlight potential scams before they become an issue. This training can be initiated in a couple of ways, each ensuring all at-risk employees have the support they need.

The first approach is to provide training during onboarding. Integrating training into the onboarding process provides the skills and awareness needed to manage risk from day one of employment. Training should focus on security best practices (CISA, n.d.), from password strength and software updates to using multi-factor authorization where appropriate.

In addition, ongoing training can be initiated using KPI metrics. Providing quantifiable data on employee performance, business outcomes, and more, employers can identify problem behaviors in individuals or highlight trends in security risk that require attention. The key is selecting appropriate KPIs to monitor, but employees should also use employee feedback to highlight areas of uncertainty (Abbas, 2023).

With this data, employers can provide the support needed to help BBC employees with appropriate training, all in a timely manner.

Device Control

Taking control of the devices accessing your network can alleviate many of the issues that scams and hacking can bring. You not only control the devices on your network, but also the software and systems running on those devices. Your team can keep them fully updated without relying on individual users, ensuring that each device has the most up-to-date protections running at all times.

This extends to how your network and data are accessed. The modern work environment means that users could be working from home, out on the road, or on location with clients. By using company-managed VPN systems and accounts, your business remains in control. You have complete visibility of all devices, what they are doing, and the data they are accessing. In turn, this empowers any protection system, providing the platform your team needs to maintain network integrity and identify new threats quickly.

Governance, Risk and Compliance (GRC) Model Application

The GRC model is ideal for managing the issues of BBCs within the workforce. By taking a methodical approach to each aspect of oversight and management, a comprehensive and effective solution can be quickly introduced.

Governance

BBCs must be encouraged at every level, and that means a commitment from leadership to protect any older employees. This means minimizing the risk of attack they face, either from device management, training, or adjusting duties to suit.

They should know that leadership supports them to maintain their productivity while minimizing exposure to potential security threats. By ensuring that onboarding and reviews incorporate the concept of cybersecurity threats, and having appropriate training programs in place, leaders provide the tools and support older employees need, and provide a visible commitment that builds trust and ensures these employees retain their sense of value within the organization.

Risk

Risk assessment must be an ongoing strategy, taking into account each individual's digital behavior and the job role they have. This type of continuous appraisal through regular risk assessments helps identify areas of vulnerability early, allowing for additional training or other strategies to avoid problems.

With careful selection of KPIs, risk trends can be easily analyzed across all employees as well as individual BBCs, allowing for rapid identification of issues and implementing preventative measures as required, whether that is training or other approaches.

Compliance

Putting policy in place to enable all the safety initiatives previously discussed ensures that all employees are given the tools and protection they need. That includes data handling policies, mandatory training for identifying and handling scam attempts, and a comprehensive set of security protocols to spot issues and deal with incursions effectively.

One area of importance is the onboarding policy. This should cover the onboarding process for both new hires as well as employees shifting to new roles. Incorporating appropriate training for identifying and avoiding scams and other cyberthreats into policies covering the onboarding process ensures that every employee is up-to-date with he skills they need to minimize risk in their current role.

Visual Table: Strategy to Overcome BBC Vulnerabilities

BBC Challenge	Scam Type	Vulnerability	Protective Strategy
Trust in unknown callers	Tech support scams	No knowledge of modern scams	Mandatory awareness training & scam reporting Hotline
Emotional isolation	Dating/romance scams	Easily manipulated emotionally	Digital literacy with emotional resilience modules
Misunderstanding of digital devices	Phishing via email	Clicks on malicious links	Spam filter training, phishing simulations
Lack of password best practices	Credential theft	Reused or shared passwords	Enforced multi-factor authentication

Conclusion

With so many BBCs still fulfilling valuable roles within the workforce, the vulnerability of employees to scams that they represent cannot be ignored. Businesses have to provide the support they need through targeted protection. This can include digital education, employer safeguards, GRC Frameworks, and more, significantly reducing risks for both the individual and organization.

Protecting this generation is not only a governance priority but also a cybersecurity necessity.

References

Abbas, T. (2023, June 25). *10 examples of KPIs for learning and development*. Retrieved from Change Management Insight: https://changemanagementinsight.com/examples-of-kpis-for-learning-and-development/

CISA. (n.d.). *Security Best Practices*. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/topics/cybersecurity-best-practices

Fry, R., & Braga, D. (2023, December 14). *The Growth of the Older Workforce*. Retrieved from Pew Research Center: https://www.pewresearch.org/social-trends/2023/12/14/the-growth-of-the-older-workforce/

Grilli, M., McVeigh, K., Hakim, Z., Wank, A., Getz, S., Levin, B., . . . Wilson, R. (2021). Is This Phishing? *Journals of Gerontology, 76*(9). Retrieved from https://academic.oup.com/psychsocgerontology/article/76/9/1711/6055602

Holt, M. (2024, December 17). *Understanding Boomer Values*. Retrieved from Divrsity: https://divrsity.team/blog74-boomers-and-dei.html#:~:text=Traditional%20Hierarchy%20and%20Respect%20for%20Authority

McDermott, R. (2012, February 1). Emotion and Security. *Communications of the ACM, 55*(2), 35-37. Retrieved from https://dl.acm.org/doi/abs/10.1145/2076450.2076462

Microsoft. (2025). *Role-based security*. Retrieved from Learn.Microsoft: https://learn.microsoft.com/en-us/power-platform/admin/database-security

Morrison, B., Coventry, L., & Briggs, P. (2021). *How do Older Adults feel about engaging with Cyber-Security?* Wiley. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/hbe2.291