

The Pitfalls of Computing

Protecting your digital life

Brian Baker

11 September 2026



The Pitfalls of Computing

Security Risks



Privacy Concerns



System Crash



Data Loss



Tech Confusion



Misinformation



Costly Upgrades



The Pitfalls of Computing

Security Risks



Privacy Concerns



System Crash



Data Loss



Tech Confusion



Misinformation



Security Risks — Unauthorised access, viruses, scams, phishing emails, and unsafe downloads can compromise your data.

The Pitfalls of Computing

Security Risks



Privacy Concerns



System Crash



Data Loss



Tech Confusion



Misinformation



Privacy Concerns — Websites and apps may collect more information than you realise.

The Pitfalls of Computing

Security Risks



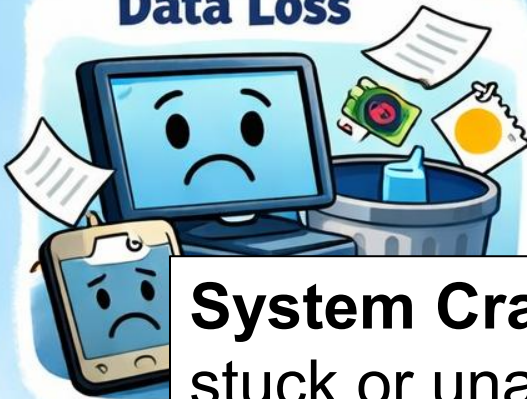
Privacy Concerns



System Crash



Data Loss



Tech Confusion



Misinformation



System Crash — When systems fail, we can be left stuck or unable to work.

The Pitfalls of Computing

Data Loss — Hardware failures, accidental deletion, or lack of backups can wipe important files.



The Pitfalls of Computing

Complexity & Confusion — Constant updates, new layouts and menus can frustrate users. Computer and internet problems.



The Pitfalls of Computing

Misinformation — Not everything online is accurate. Scams and false information spread easily. Fake news. Searches and AI do not always provide accurate information.



The Pitfalls of Computing

Cost of Upgrades — Keeping devices, software, and security tools up to date can be expensive. Old devices often will not support latest versions of software.



Key Points

- **Security Risks** — Unauthorised access, Viruses, scams, phishing emails, and unsafe downloads can compromise your data.
- **Privacy Concerns** — Websites and apps may collect more information than you realise.
- **Over-Reliance on Technology** — When systems fail, we can be left stuck or unable to work.
- **Data Loss** — Hardware failures, accidental deletion, or lack of backups can wipe important files.
- **Complexity & Confusion** — Constant updates, new layouts and menus can frustrate users. Computer and internet problems.
- **Misinformation** — Not everything online is accurate. scams and false information spread easily. Fake news. Searches and AI do not always provide accurate information.
- **Cost of Upgrades** — Keeping devices, software, and security tools up to date can be expensive.

Security



Why Security Matters

- Laptops, tablets and smartphones store personal and sensitive data
- Good security reduces the risk of data loss and misuse
- Digital crime (Cybercrime) comes in many forms including:
 - Malware or malicious and unwanted code
 - Viruses (requires human to trigger it)
 - Worms (self-replicates)
 - Trojans (disguises itself as a legitimate, useful or harmless software)
 - Phishing (email), Vishing (voice), Smishing (SMS/text), Quishing (QR code phishing) and ClickFix (deceptive social engineering techniques)
 - Finfluencers (financial influencers)
 - Identity Theft
 - Credit Card Theft/Fraud
 - Spoofing (imitation of something trusted to trick you into handing over sensitive information)
 - Denial of Service (caused by overwhelming amounts of traffic)
 - Sniffing (e.g. eavesdropping)
 - Ransomware (highly destructive malware that encrypts or locks your files)
 - System Failures (e.g. Software design flaws).

Passwords

How secure is my password - Quiz #1

According to security.org (<https://www.security.org/how-secure-is-my-password>) and <https://bitwarden.com/password-strength/>, which of these passwords would take a computer the longest to crack?

- ^damDun!0p
- Br!anBak3r
- G3offCorb3tt
- J0hn<r055
- Lynda\$3ar5
- \$u3Ha1f0rd

Passwords

How Secure is My Password - Quiz #1

According to security.org (<https://www.security.org/how-secure-is-my-password>) and <https://bitwarden.com/password-strength/>, which of these passwords would take a computer the longest to crack?

	<i>security.org</i>	<i>bitwarden.org</i>
— ^damDun!0p	5 years	12 days
— Br!anBak3r	5 years	3 seconds
— G3offCorb3tt	2,000 yrs	5 hours
— J0hn<r055	1 month	26 seconds
— Lynda\$3ar5	5 years	4 hours
— \$u3Ha1f0rd	5 years	2 hours

Passwords

- In theory you can use up to 95* different characters in a typical password
- These are the characters most systems allow:
 - 26 lowercase letters (a–z) and 26 uppercase letters (A–Z)
 - 10 digits (0–9)
 - 33 symbols (punctuation and special characters such as ! @ # \$ % ^ & * () _ + etc.)
- Total: 95 characters
- Why length matters
 - Password strength grows exponentially with the number of characters in the pool:
 - A password using all 95 characters has a much larger search space than one using only letters or letters+numbers.
 - But length matters far more than character variety — adding one extra character increases strength more than adding symbols.
- What Is a Good Password Length? (NIST 2026 Guidance)
 - The short answer: 16 characters for accounts, 20 or more for anything high-value, and treat 8 as obsolete. Sixteen random characters put a password permanently beyond brute force while fitting every mainstream service.

* Some systems reduce the number to 88

Passwords

Made with AI



Paaswords

- For a fully random password using uppercase, lowercase, numbers, and symbols (an 88-character pool), here is what each length buys against an offline attacker testing 10 billion guesses per second:
 - 8 characters - about 3 days
 - 10 characters - about 58 years
 - 12 characters - hundreds of thousands of years
 - 14 characters – longer than the age of the universe
 - 16 characters - longer than the age of the universe
 - 20 characters - longer than the age of the universe

Paaswords

Passwords – Quiz #2

- If a 16-character password takes longer than the age of the universe to crack, why does NIST 2026 guidance recommend 20 or more characters for anything of high value?

Paaswords

Passwords – Quiz #2

- If a 16-character password takes longer than the age of the universe to crack, why does NIST 2026 guidance recommend 20 or more characters for anything of high value?
- Because *real-world attackers don't brute-force from scratch*.
- A **fully random** 16-character password *is* effectively uncrackable — but **most 16-character passwords humans create are not random**, and NIST's guidance is designed for *human behaviour*, not mathematical perfection.
- Modern cracking doesn't start at 0 — it starts with billions of known passwords
 - NIST's 2024–2026 guidance **emphasises screening against breached password because attackers begin with:**
 - billions of leaked passwords
 - wordlists
 - mutation rules
 - AI-generated guesses
 - personal data (names, pets, dates).

Passwords

- There are lots of free password strength checkers (and they produce different results):
 - security.org <https://www.security.org/how-secure-is-my-password/>
 - bitwarden <https://bitwarden.com/password-strength/>
- There are websites that will check if your password or email address has been exposed in a data breach:
 - Have I been Pwned <https://haveibeenpwned.com/>

How to Spot a Scam Website

- Why spotting scam websites matter
 - Scam sites steal money, personal details, or passwords
 - They often look professional and convincing
 - Knowing the red flags helps you stay safe
- Check the Website Address (URL)
 - Look for misspellings (amaz0n, barclays-secure-verify).
 - Avoid sites with extra words (paypal-login-confirm-now).
 - Be cautious of unusual endings: .xyz, .top, .info.
 - Make sure it starts with https:// and shows a padlock.
- Look for Professional Quality
 - Spelling mistakes
 - Blurry logos
 - Poor layout
 - Broken English
 - Missing pages (About, Contact, Terms)

How to Spot a Scam Website

- Beware of “Too Good to Be True” Offers
 - Extremely low prices or huge discounts
 - “Only 3 left — buy now!”
 - Free gifts for entering your details
- Check Contact Information
 - Legitimate sites provide:
 - Address, Phone number, Email, Customer service details
 - Scam sites often have none, or only a web form
- Watch for Suspicious Payment Methods
 - Avoid sites that ask for:
 - Bank transfer
 - Gift cards
 - Cryptocurrency
 - Safe sites use:
 - Credit/debit cards
 - PayPal
 - Trusted payment gateways

How to Spot a Scam Website

- Check Reviews Before You Buy
 - Search online:
 - “Website name + reviews”
 - “Is <website> legit”
 - Fake reviews often look repetitive or overly positive.
- Watch Out for Pop-ups and Urgent Messages
 - Examples include:
 - “Your computer is infected!”
 - “You’ve won a prize!”
 - “Verify your identity now!”
 - These are designed to panic or pressure you.
- Trust Your Instincts
 - If something feels odd, rushed, or too good to be true, stop and close the page.
- Quick Checklist
 - ✓ Correct URL ✓ HTTPS padlock ✓ Professional design ✓ Real contact details ✓ Sensible prices ✓ Genuine reviews ✓ No pressure tactics

How to Spot a Scam Website

- To check if a website is a scam, paste its URL into a reputation tool like urlvoid.com
- Search the domain on a WHOIS lookup tool like who.is and look at domain age.
- If the site was registered only a few weeks or months ago, it is likely a scam

- If you've seen something that doesn't feel right, STOP!
 - break the contact – don't click on any links or make any payments
 - check if it's genuine: compare the domain name (web address) with one you know to be real
 - look at reviews from several online review sites, for example Trustpilot, Feefo or Sitejabber
 - report it to the [National Cyber Security Centre](https://www.ncsc.gov.uk) (NCSC)

How to spot an email scam

- 1. Check the sender's email address
- 2. Is the greeting impersonal?
- 3. Check contact information and dates
- 4. Check the branding
- 5. Check if the linked website is legitimate
- 6. Is the email asking for personal information or bank details?
- 7. Does it have poor spelling, grammar and presentation?
- 8. Is it trying hard to be 'official'?
- 9. Is it trying to rush you?
- 10. Check with company, brand or department

Example Scam Email (for training purposes, clean version)

From: security-update@halifaxsecure-alerts.com

Subject: URGENT: Your Account Has Been Limited – Immediate Action Required

Dear Customer,

We have detected unusual activities on your Halifax account on 17/13/2026.

To protect your safety, we have temporarily limited your account.

Please verify your details within 12 minutes to avoid permanent suspension.

Click the link below to restore full access: <http://halifax.verify-account-secure-login.com>

As part of our new security protocols, you must confirm:

- Your full name
- Address
- Date of birth
- Bank card number and 3-digit code

Failure to comply will result in your account being terminated and funds withheld.

Thank you for your cooperation, Halifax Security Team Halifax Inc., 123 Web Street, London, UK, 00000

© 2026 Halifax. All rights reserved.

Example Scam Email (for training purposes – with comments)

From: security-update@halifaxsecure-alerts.com

[1. Suspicious sender address — looks like Halifax but isn't]

Subject: URGENT: Your Account Has Been Limited – Immediate Action Required

[9. Trying to rush you]

Dear Customer,

[2. Impersonal greeting]

We have detected *unusual activites* on your Halifax account on **17/13/2026**.

[3. Incorrect dates + errors]

To protect your safety, we have *temporarily limited* your account.

Please verify your details within **12 minutes** to avoid *permanent suspension*.

[9. Pressure + urgency]

Click the link below to restore full access: ➡ <http://halifax.verify-account-secure-login.com>

[5. Fake website — looks similar but is not Halifax]

As part of our new security protocols, you must confirm:

- Your full name
- Address
- Date of birth
- Bank card number and 3-digit code

[6. Asking for personal and financial information] and [7. Incorrect spelling 'protocols']

Failure to comply will result in your account being terminated and funds withheld.

[8. Overly "official" threats]

Thank you for your cooperation,

Halifax Security Team Halifax Inc., 123 Web Street, London, UK, 00000 [3. Fake or incorrect contact details]

© 2026 Halifax. All rights reseved.

[7. Poor spelling, grammar, and presentation]

Genuine Email Example

From: service@halifax.co.uk

Subject: Important Information About Your Halifax Account

Hello Brian,

We're writing to let you know about a recent login from a new device.

If this was you, no action is needed. If not, please visit halifax.com and go to **Settings** → **Security** to review your recent activity.

For your safety, please remember:

- We will never ask for your bank card number or security code by email
- We will never threaten to close your account
- We will never ask you to click a link to “verify” your identity

If you need help, contact us through the **Help Centre** on the official Halifax website.

Thank you for using Halifax, The Halifax Team, Halifax, 6 Trinity Road, Halifax, West Yorkshire, HX1 2RG.

© 2026 Halifax. All rights reserved.

How do spot a text message scam

1. Sense of urgency or threat
“Suspended”, “Permanent closure”, “2 hours” — designed to panic you
2. Unexpected contact
Banks, HMRC, NHS, mobile networks etc. don’t text out of the blue asking for verification
Hi Mum or Hi Dad, Recruitment agencies etc.
3. Fake link that looks almost right
Looks similar but is wrong
4. Pressure to click on a link
Real banks tell you to use the official app or website
5. Suspicious phone number
Scam numbers often use 0845 / 0870 / random mobiles.
6. Generic greeting
No name, no partial account number — a real bank would personalise
7. Poor formatting or tone
Overuse of capitals, strange phrasing, pushy language
8. Pretending to be a trusted brand
Pretends to be Barclays to gain trust

Example Scam Text (for training purposes, clean version)

URGENT: Your Barclays account has been SUSPENDED due to unusual activity.

To avoid permanent closure, verify your identity within the next 2 hours.

Visit secure link:

barclays-verify-secure-123.com/login

Failure to act will result in **account restrictions** and **loss of access**.

For assistance, call our security team immediately on **0845 229 7714**.

Barclays Security Team



Example Scam Text (for training purposes – with comments)

URGENT: Your Barclays account has been SUSPENDED due to unusual activity.

[2. Unexpected contact]

[6. Generic greeting]

To avoid permanent closure, verify your identity within the next 2 hours.

[1. Urgency & threats]

Visit secure link:

barclays-verify-secure-123.com/login

[3. Fake link that almost looks right]

[4. Pressure to click a link]

Failure to act will result in **account restrictions** and **loss of access**.

[7. Poor formatting and tone]

For assistance, call our security team immediately on **0845 229 7714**.

[5. Suspicious phone number]

Barclays Security Team

[8. Pretending to be a trusted brand]



Example of a Vishing Phone Call

“This is your bank’s fraud department.

We have detected some unusual activity on your account – a payment of £199 to Amazon and a payment of £1,199 for a foreign bank transfer.

If you did not make this payments, please press “1” to speak to our fraud prevention team.”

Key Warning Signs

- Scare tactics and urgency
- Pressure not to hang up
- Action confirming phone number belong to a human
 - Will lead to requests for sensitive information (card number, security code)
- Pretending to be from a trusted organisation (but clearly saying which)
- Legitimate banks never ask for full card numbers, PINs, or security codes over the phone.

What do I do if I receive a scam email or text?

- **Scam Emails**

- Simply forward to :
- report @phishing.gov.uk
- (then delete)

- **Scam Texts**

- Simply forward to :
- 7726
- then delete; do not engage

- **Scam Calls**

- Do not engage if number not recognised
- BLOCK number-
- Phone 1 5 9 to talk to your bank (via a switchboard)

What to do if you fallen victim to a scam

- Disconnect your computer from the internet
 - Turn off wi-fi or unplug the Ethernet cable, as this can prevent malware from sending or receiving data
- Run a malware scan
 - Use your antivirus. If you don't have one installed, on Windows 10 or 11, search for Windows Security, then go to Virus & threat protection > Scan options > Full scan
 - This checks the files and programs on your computer for threats
- Don't sign in to important accounts
 - Until you're confident your computer is clean, don't use it to access your email, online banking or other important accounts
 - Some malware is designed to steal passwords and personal information.
- Change your passwords using another device
 - On a trusted phone, tablet or computer, change the passwords for your most important accounts, starting with your email
 - Use unique passwords and turn on two-factor authentication where it's available

What to do if you fallen victim to a scam

- Check your accounts for suspicious activity
 - Look through your bank accounts and other important services for payments, logins or other activity you don't recognise
 - Contact your bank immediately if you spot anything suspicious.
- Report the scam - You can report the scam to:
 - Action Fraud: Submit details about the scam to Action Fraud
 - GOV.UK: Report the scam online or by calling 0300 123 2040
- If you're concerned that malware might be installed on your computer, see expert advice.

Backup Slides



Passwords

- Passwords

- Websites determine minimum and maximum length and required combination of uppercase, lowercase, numbers or symbols
- Dos and Don'ts:
 - Don't use personal information
 - Don't use words found in the dictionary
 - Length is stronger than complexity
 - Recommended length is at least 12 characters, with 14 – 16+ being better.
 - Don't use the same password for every account
 - Use a combination of uppercase, lowercase, numbers or symbols depending on what is allowed
 - Use a phrase that you can remember and take the first letter from each word.
- Suggestions
 - Add or replace a letter with a number, e.g. replace e with 3 (Baker > Bak3r)
 - Add or replace a letter with a symbol, e.g. Replace i with ! (e.g. Brian > Br!an)
 - BrianBaker would take a computer about 1 month to crack
 - Br!anBak3r about 5 years
 - TheCatSatonthMat about 1 hundred billion years.

Passwords

- Changing Passwords
 - If you think someone knows your password, go into your account and change it
 - If you change your password, you should get an email telling you that has happened
 - If you get an email that says you have hanged your password and you haven't, someone else may have changed it
- Passwords are stored remotely:
 - Passwords are therefore transmitted across networks and the internet
 - https: makes passwords significantly safer by encrypting data in transit between your browser and the website server, preventing hackers on the same network from eavesdropping.
 - If a site is not using https:
 - preferably do not use it
 - If you do use it, do not use public Wi-Fi (unless you use a VPN)
- Security of passwords also depend on the website:
 - Poorly implemented websites might store your website in plain text or poorly encrypted
 - Passwords will not be protected if the website's database is breached
 - If using a public computer always ensure you do not save your password and log out.

Passwords

- Places you should **NOT** store your passwords
 - Plain text documents on your computer
 - Easy to find if someone gains access to your computer
 - It's common for people to keep other sensitive information in the same file
 - An unlocked laptop
 - Leaving a laptop unattended and unlocked can be enough for someone to access your passwords or copy sensitive information
 - Adjust how quickly your screen turns off
 - Make sure your laptop locks itself automatically so that a password is required after waking from sleep
 - In an email (e.g. to yourself)
 - Email accounts are one of the most valuable targets for cybercriminals
 - Unprotected notes on your phone (e.g. Notes app)
 - Risk of theft or of being lost
 - If you do, make sure you lock the Note
 - Shared cloud storage folders
 - Useful for accessing your files from anywhere but make sure the file is not shared
 - Unencrypted USB sticks
 - Risk of theft or of being lost.

Passwords

- Where should I store my passwords
 - Password Notebook
 - Dedicated notebook kept in safe or hidden in a secure location away from your computer
 - Keep usernames and accounts in a separate location from passwords
 - Use a memory cipher (e.g. add complex or long phrase and add a unique element for each website)
 - Secure Local File
 - Password protected file such as a Word document or Excel spreadsheet
 - Ideally encrypted or using a logical formula
 - Browser Storage (Built-in)
 - Google Chrome Password Manager (Menu > Passwords and Autofill > Password Manager)
 - Microsoft Edge Password Manager (Settings > Profiles > Passwords)
 - Third-Party Password Manager
 - 1Password, Bitwarden, Proton Pass, LastPass and many more
 - Free password managers are usually feature-limited versions of their premium password managers.

Passwords

- In 2025, the most common passwords continue to be dominated by weak, easily guessed, and numerical sequences, with "123456" remaining the top global choice, while "admin" and "password" dominate in the UK and US
- These predictable, and often reused, credentials are responsible for 80% of data breaches
- Top 20 Common Passwords 2025 (UK/Global Trends):

- | | | | |
|--------------|---------------------------|-----------------|-----------------|
| 1. 123456 | 6. Password1 | 11. Password123 | 16. 123qwe |
| 2. admin | 7. Password (capitalized) | 12. Fortnite21 | 17. abc123 |
| 3. password | 8. 12345 | 13. password1 | 18. Strongman12 |
| 4. 12345678 | 9. Lennon11 | 14. qwerty123 | 19. daday123 |
| 5. 123456789 | 10. 1234567890 | 15. qwerty | 20. Liverpool1 |

