Cyber Awareness Month: Vulnerabilities beware this Halloween

BY ELEANOR BARLOW · OCTOBER 27, 2025 · LAST UPDATED ON DECEMBER 24, 2025

What you will learn

- **Common cyber threats around Halloween:** Learn how seasonal scams, phishing, fake event promotions, and fraudulent sites exploit holiday shopping and activities.
- **Hidden risks like dormant accounts and insecure IoT devices:** Understand how unused profiles and poorly secured gadgets can become entry points for threats.
- **Practical safety tips:** Get simple, actionable cybersecurity advice, from using MFA and secure networks to avoiding fake links and oversharing online.

Cybersecurity Awareness Month: why it matters and this year's theme.

We couldn't let Cybersecurity Awareness Month slip by without posting a bit of a fun blog on the topic, with a Halloween twist!

Launched by the National Cybersecurity Alliance and the U.S. Department of Homeland Security in 2004, Cybersecurity Awareness Month was formulated to encourage, as well as provide people with the right tools to protect themselves against cyber threats.

Each year, a different theme is selected to support online safety. For 2025, the topic of 'Staying safe online' was selected. To support, the NCA has provided information on four core segments covering the importance of:

1. Strong passwords
2. Multifactor authentication
3. How to report scams
4. How to update software

To further assist the 'Staying safe online' initiative and, with it, the necessity of strong passwords, multifactor authentication, the importance of updates, and how to report a threat, this blog takes a look at some of the cyber threats and how to safeguard against them.

Halloween outfits with a real scare factor

Last-minute Halloween costume shopping can be more frightening than you expect, especially when it comes to online purchases.

Fraudulent websites, designed to trick shoppers with malicious links and credential-stealing scanners, often lure buyers with tempting promotions, like “50% off fangs for less”. But behind these offers can lie links leading to phishing scams aiming to trick you into a fraudulent deal and/or harvest your personal information.

CheckPoint confirms that there has been a 160% rise in compromised credentials so far this year. One major reason is the advancement of AI, which has made phishing attacks more sophisticated and accessible. Gone are the days of obvious typos and poor formatting that would give a phishing email away; AI-generated phishing emails now look highly convincing, allowing even inexperienced threat actors to launch malware or ransomware campaigns. In fact, with malware-as-a-service and ransomware-as-a-service available on the dark web, anyone with malicious intent, some form of payment, and some basic knowledge of the dark web can initiate a cyberattack.

‘Late last year, we reported 14,000 cases in just 1 month where our customers’ employee credentials, even those adhering to company password policies, were exposed in data breaches – a clear indicator of real and present risk.’ – **Checkpoint**

To protect yourself when buying Halloween costumes (or anything, for that matter) online, remember to:

1. Purchase only from reputable and well-known retailers.
2. Access websites directly by typing the URL out yourself, never through links in emails or social media. And to download apps, go to the app store directly.
3. Use a credit card instead of a debit card for added fraud protection with online purchases.
4. Enable two-factor authentication (2FA) on your accounts whenever possible.
5. Keep your devices’ security software updated to detect and block malicious sites and malware.

Charity frights

Around this time of year, not only do costume stores, promotions, and fraudulent emails increase, but so do Halloween-themed events. A tempting promotion, advertisement, or even QR code might draw you into a murder mystery or mansion party. However, once you enter your credentials and complete payment, your ticket can suddenly disappear without a trace.

Charity events are also a common target for scams during Halloween. You might come across fundraisers with a Halloween theme, such as contests to vote for the best costume, claiming that all profits go to a good cause. The frightening truth is, you may never realize you’ve been scammed, since there’s no way to track where your money goes.

We probably don’t need to tell you this, but as it’s awareness month, here are some reminders to stay safe online:

1. As always, never share personal information with untrusted sources.
2. Do your research before participating and check the charity registration number/code.
3. When in doubt, ask the charity directly for more information.

Dormant profiles and zombie accounts

While not specific to Halloween, a zombie account is any account that is still active but unused. These accounts often sit on old devices and systems and can be used as a gateway to launch attacks, such as credential stuffing attacks, where information from data breaches is used to log into accounts.

Secure Data Recovery showed that '94% of respondents admitted to having one or more zombie accounts - accounts left unused for at least 12 months.'

It's not just on personal devices. Dormant business accounts are low-hanging fruit that companies need to be mindful of. Equally, companies need to consider former employee access levels and update account logins and MFA regularly.

'Dormant accounts represent 24.15% of all accounts for an average enterprise. [...] 79.87% of application accounts go unused every month, highlighting that users have access to too many applications and sensitive data.' - blog from Oort

The best way to handle dormant accounts is to deactivate them. Many people mistakenly think deleting an app from their phone removes their account, but unless you deactivate it, your account still exists online and can be used as an entry point to other accounts.

Hardware with a scare

Many celebrations feature bright lights, lively music, and devices that create eye-catching visual effects. However, these gadgets are often only unboxed for a single occasion, which means proper security controls are rarely in place.

Consider Internet of Things (IoT) devices such as Halloween lights or decorations, smart speakers, and music systems. These are typically left with their default password settings, making them an easy entry point for potential attacks.

There are, according to SQ Magazine, '18.8 billion active IoT devices worldwide', and 'the average data breach cost for IoT-related incidents is $2.17 million'.

Keep your Halloween sweet with these 8 tips, not tricks!

1. **Zero trust**: Assume everything has malicious intent. Do not trust links, promotions, emails, QR codes, or events without verifying authenticity. Always do your due diligence before providing information.
2. **MFA enablement**: Multifactor authentication is a must for all digital accounts. Build layers between your data and the threat actors trying to ruin your celebrations.
3. **Ignore urgency**: If the Halloween offer runs out in one hour, or that vampire outfit is 85% off for the next two days, it might just be fraudulent. Type URLs manually and avoid any promotions using urgency as a tactic.
4. **Update software**: Keep devices, browsers, and systems updated to maintain security and performance.

5. **Avoid scam bots**: AI-generated support systems are not always what they seem. Verify that you are on an official site before engaging with live or virtual chatbots, which are there to steal information.
6. **Bank safely**: If you purchase Halloween supplies online, make sure to do so with a credit card, not a debit card, as most credit card providers protect their customers from fraudulent activity.
7. **Secure Wi-Fi:** Don't log into sensitive accounts (banks, socials, payment gateways), while on public Wi-Fi. Use a secure, private network for any transactions.
8. **Oversharing media:** Be mindful of what you share online. Not just regarding the data you share, but, in the lead up to Halloween, travel plans, party times/locations advertised on socials in real time can make it easier for scammers to commit fraud.

This spooky season, don't let digital threats haunt your business. For expert tips and tailored strategies on building a robust bug bounty program, get in touch with our team today.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com