Essential Cybersecurity Takeaways

This article will provide you with some insights and essential cybersecurity takeaways from experts in the sector to how be better protected when using the internet.

Introduction

It is common to assume that cybercrime/network intrusions are carried out by a hacking expert sat at a computer with the command line up, breaking in through technical means. In reality, though, this is really hard! This document details the main principles that everyone should adopt in their day-to-day lives when navigating the cyber world and includes pointers on **Phishing**, **Password Security**, and **Data Breaches**.

Your **awareness** is your strongest defence. When you understand an attacker's tactics, you move from being a potential victim to an active protector of your data and your network.

1. Phishing: The Art of the Psychological Trap

Phishing remains one of the most successful methods attackers use to gain access to sensitive information. It is essentially a digital form of social engineering, preying on human psychology to trick users into clicking a malicious link, downloading an infected file, or revealing credentials.

Five core psychological triggers can be highlighted that phishers exploit. Recognizing these levers is the first step toward successful defence:

- **Control/Authority:** Posing as a superior, manager, or IT technician (a figure of authority) to induce immediate compliance without questioning.
- **Urgency:** Creating a false sense of crisis (e.g., "Your account will be suspended in 10 minutes!") to bypass rational thought and force a quick, reactive click.
- **Recent Events:** Referencing current events such as "Please donate to help the refugees in Ukraine" or a popular one at the time "Click here to book your COVID vaccine" or company-specific news to make the email seem timely and relevant.
- **Scarcity:** Suggesting a limited opportunity (e.g., "Only 3 spots left for this mandatory training," or "Final warning for this offer") to encourage impulsive action.
- **Emotion:** Playing on strong feelings like fear, greed, curiosity, or desire to help, clouding judgment and making the user less likely to scrutinize the sender.

Defending Against Phishing Attacks

The key defence is **scepticism**. Before you click, ask these four critical questions:

- **Is the Sender Correct?** Check the sender's actual email address, not just the display name. A slight misspelling of a company domain (e.g., support@micros0ft.com) is a huge red flag.
- **Is the Tone Appropriate?** Urgent, overly aggressive, or emotionally charged requests are highly suspicious, especially if they demand money or information immediately.
- **Check the Link (Hover, Don't Click):** Before clicking any hyperlink, hover your mouse over it (or press and hold on mobile) to view the destination URL. If the link destination doesn't match the context (e.g., a "Google Drive" link goes to a random address), do not click. This can unfortunately now be spoofed so extra care must be taken.
- **Beware of Unusual Attachments:** Files ending in extensions like **.exe**, **.zip**, **.js**, or document files that require you to "Enable Content" (like a **.docm** macro file) should be treated as high risk. If you weren't expecting it, don't open it.

2. Password Security: Your Digital Lock

Your password is the primary lock on your digital life. Attackers employ various methods to break these locks, making strong password hygiene a must.

The Attack Methods

- **Dictionary Attack:** The attacker uses a list of common words, phrases, and simple variations (like substituting "s" for "$") against a system.
- **Targeted Attack:** An attacker uses knowledge about you (names of pets, birthdays, schools, etc. often taken from social media) to create specific, personalised guesses. **Easy-to-find personal information** should **never** be used in a password.
- **Brute Force Attack:** The attacker uses software to systematically try every possible combination of characters until the correct password is found. This is where **password length** becomes the most powerful defence.

The Power of Length and Randomness

The following illustration of crack times proves that **length and a few random elements** are vastly superior to simple complexity rules:

Example Password	Time to Crack	Takeaway

grinning123	3.6 seconds	Too short, common word, easy sequence.
Gr!nNiNg123	11.5 minutes	Capital letters and symbols provide minimal defence when the base is short and common.
GrinningSkydivingOtter	**24 years**	**Significant Jump:** Length and randomness from three random words dramatically increase time.
GrinningSkydivingOtter£33	**20 million years**	**Near Impenetrable:** Extreme length with mixed characters is the gold standard.

The New Standard: Three Random Words & Password Managers

The single most effective strategy is the **three random words method**. Instead of trying to memorize a complex, short string, create a long, memorable passphrase by combining three completely random, unrelated words (and optionally adding a number or symbol): PillowLakeSatellite7£.

The Necessity of using a Password Manager:

To ensure every online service has a unique, long, and complex password, **using a password manager** is strongly advised. These tools securely generate and store unique, high-entropy passwords for you. This means if one service is breached, your password for every other site remains safe.

3. Data Breaches: Why Unique Passwords Matter

The reality of **Data Breaches** is a key concern. A data breach occurs when a cybercriminal successfully exploits a vulnerability in an organization's network, gaining unauthorised access to, and stealing, customer or employee data.

Minimising Your Exposure

1. **Unique Passwords for Everything:** This is the *only* way to make a data breach on a third-party site irrelevant to your other accounts. Use a password manager to enforce this.
2. **Limit Data Sharing:** Be cautious about how much personal information you provide to non-essential services. Less data shared means less data potentially exposed in a breach.

3. **Enable Two-Factor Authentication (2FA) Everywhere:** For all critical accounts (email, banking, social media), enable 2FA. Even if an attacker steals your password, they cannot log in without the one-time code generated by your phone.

By adopting strong habits, using a password manager, creating long passphrases, and maintaining a high level of skepticism toward suspicious communications, you are closing the digital doors that attackers try to force open.

Please answer to these questions it will only take less than 1 minute:

1. How likely are you to change your password after reading the article? (1 being really unlikely – 10 being highly likely)
2. Was the article useful? (1 being not useful at all – 10 being extremely useful)
3. Would you like to hear more information on online security? Yes/No
4. Any other comments?