ONLINE SECURITY GUIDE

TIPS TO KEEP YOU SAFE AND SECURE

THE HOME OF
MARTIAL ARTS BUSINESS

NEST

www.nestmanagement.co.uk

ONLINE SECURITY GUIDE

TOP TIPS

HOW TO STAY SAFE ON GOOGLE ADS

Activate Two-Factor Authentication (2FA):

- Add an extra layer of security to your Google accounts by activating two-factor authentication.
- Any changes to your account will need to be confirmed using two-factor authentication before being implemented.

Beware of Email Scams:

- Google only communicates through official emails ending in @google.com.
- Be cautious of emails from Gmail accounts or other domains claiming to be Google, these are scam accounts and are not safe.

Verification of Google Calls:

- If Google contacts you by phone, ensure they confirm the first 6 digits of your account number.
- Legitimate calls from Google will provide these account details. If the caller cannot confirm your account number, treat it as a potential scam.

PASSWORDS

Change Passwords Periodically:

- Enhance security by changing passwords regularly.
- Ensure that the new password is unique and not easily guessable.
- Consider changing them more frequently than prompted.

Unique Passwords for Each Account:

- Use strong, unique passwords for every online account.
- Avoid using the same password across multiple platforms.

PHISHING

Phishing is a deceptive technique used by scammers to obtain your personal information. Scammers may impersonate friends, banks, or colleagues to trick you into revealing sensitive details.

- Does the email look poorly written, contain spelling mistakes, or seem unlike the usual communication from that person?
- Did the email come out of nowhere, and you were not expecting it?

GENERAL ADMIN

Be Cautious with Links:

Avoid clicking on suspicious links in emails or messages.

Double-check the URL before entering login credentials or personal information.

Update Software Regularly:

Keep operating systems, antivirus, and applications up to date. Regular updates often include security patches.

NEST

ONLINE SECURITY GUIDE

TOP TIPS

HOW TO STAY SAFE ON FACEBOOK ADS

Beware of Communication/Email Scams:

- Facebook will not contact you through direct messages, from unfamiliar accounts, or tag you in posts regarding account issues.
- Facebook will only communicate with you through the email address listed on your Facebook account.
- Legitimate emails from Facebook will come from the official address ending in @facebookmail.com.

Activate Two-Factor Authentication (2FA):

- Enable Two-Factor Authentication for your Facebook account, Facebook Ads account, and Facebook Business Manager.
- This adds an extra layer of security, as any changes to your account will need to be confirmed using two-factor authentication before being implemented.

Receive Notifications for Unrecognised Logins:

- Turn on notifications for unrecognised logins on Facebook.
- You will receive an alert if a new device tries to access your Facebook account, either through text or within the Facebook app, which you must approve.
- This ensures that you have control over the security of your account.

PASSWORDS

Protect Your Password:

- Never write your password down or store it online.
- Do not share your password with anyone else.

Enhance Password Strength:

- Combine two random words with a number between them.
- Change the case of some letters and insert special characters or substitute numbers (e.g. compliance becomes C0mPl1@nCe).
- Consider using a password based on a song title or other phrase.

PHISHING

Phishing is a deceptive technique used by scammers to obtain your personal information. Scammers may impersonate friends, banks, or colleagues to trick you into revealing sensitive details.

- Are you asked to click on a link within the email?
- When you click on the email address, does the actual address look authentic or does it appear suspicious despite a seemingly legitimate display name?

GENERAL ADMIN

Monitor Account Activity:

Regularly review your account activity and set up notifications for unusual logins or transactions.

Guard Personal Information:

- Avoid sharing sensitive information like passwords or financial details over the phone or online.
- Be sceptical of unsolicited requests for personal information.

NEST