

NETT-ZERO FARMERS ACADEMY

CYBERSECURITY, ONLINE SAFETY AND FRAUD PREVENTION GUIDELINES

1. Introduction

As the Nett-Zero Farmers Academy increasingly uses the internet, digital devices, electronic communication platforms, and online systems to support agricultural training, farming activities, business operations, and stakeholder engagement, the risk of cybercrime and online fraud continues to grow.

Cybercriminals and fraudsters are becoming increasingly sophisticated in their efforts to deceive individuals and organisations into clicking on suspicious links, downloading malicious attachments, sharing confidential information, or making unauthorised payments. These activities can expose the Academy, its farmers, trainees, employees, partners, suppliers, and beneficiaries to financial losses, identity theft, data breaches, and reputational damage.

Fraudsters may impersonate the Nett-Zero Farmers Academy, its management, employees, trainers, agricultural partners, funders, suppliers, or other legitimate organisations. They may create fraudulent websites and social media accounts, distribute misleading emails and messages, or make telephone calls requesting money or sensitive information. In some cases, criminals use genuine names, logos, photographs, documents, and programme information to make their communications appear authentic.

The Nett-Zero Farmers Academy recognises the importance of cybersecurity, data protection, and fraud prevention in maintaining trust and safeguarding the people and resources associated with its activities. The Academy encourages all staff, farmers, trainees, partners, and other stakeholders to remain vigilant and adopt responsible digital practices.

This guideline provides an overview of common cyber threats and practical measures to help protect individuals, agricultural businesses, farming operations, and the Academy against cyberattacks and fraudulent activities.

2. Understanding Cybersecurity Threats

Any individual, farming enterprise, educational institution, or organisation can become a target of cybercriminals. Farmers and agricultural organisations may be particularly vulnerable when using digital platforms to access training opportunities, apply for funding, purchase agricultural inputs, communicate with suppliers, or receive programme-related information.

The following are some of the most common cybersecurity threats.

2.1 Malicious Emails, Messages and Websites

Emails, SMS messages, and social media messages that appear to come from banks, government departments, agricultural suppliers, funding institutions, or the Nett-Zero Farmers Academy may be attempts to steal personal information or money.

Phishing occurs when criminals send deceptive communications or create fraudulent websites designed to trick people into revealing confidential information, including passwords, banking details, identity numbers, and other personal data.

Phishing messages may contain urgent requests to confirm account details, claim agricultural grants, register for training, receive farming equipment, or pay registration fees. Some may contain links or attachments that install malicious software on a device.

Before responding to any request, carefully check the sender's details and independently verify the legitimacy of the communication.

2.2 Malware and Ransomware

Malware is software designed to damage devices, steal information, monitor activity, or provide unauthorised access to computer systems and mobile phones.

Ransomware is a form of malware that locks or encrypts files and demands payment to restore access. Such attacks can prevent farmers from accessing important records, including financial information, production data, farm management records, training materials, and customer or supplier information.

Individuals and organisations should avoid downloading unknown files, opening suspicious attachments, or installing software from untrusted sources.

2.3 Password Theft and Unauthorised Account Access

Cybercriminals may steal passwords and use them to access email accounts, social media profiles, online banking services, and other digital platforms.

Using the same password across multiple accounts increases the risk that one compromised account could lead to others being accessed.

Staff, farmers, trainees, and other stakeholders should use strong, unique passwords for their accounts and enable multi-factor authentication wherever available.

2.4 Social Media Impersonation

Fraudsters may create fake Facebook pages, WhatsApp accounts, LinkedIn profiles, or other social media accounts that falsely represent the Nett-Zero Farmers Academy, its representatives, or its partners.

These accounts may advertise fake agricultural training programmes, scholarships, grants, employment opportunities, farming inputs, equipment, or financial assistance.

Criminals may also take control of genuine accounts and use them to request money or distribute fraudulent messages.

Always verify that an account or communication is legitimate before sharing information, making payments, or relying on announcements about Academy programmes.

2.5 Recruitment, Training and Funding Scams

Fraudsters may falsely claim to represent the Nett-Zero Farmers Academy or its partners when advertising employment, learnerships, internships, farmer development programmes, training courses, bursaries, grants, or funding opportunities.

They may request payment for registration, application processing, selection, accreditation, certificates, equipment, or the release of funds.

The Academy's official communication channels should be used to verify all opportunities and associated payment requests. No individual should assume that an opportunity is genuine merely because it carries the Academy's name or logo.

The Academy should communicate its approved fees and payment procedures through its official channels. Any request for money that falls outside these procedures should be independently verified before payment is made.

2.6 Agricultural Procurement and Supplier Fraud

Agricultural businesses may be targeted by criminals impersonating suppliers, buyers, contractors, transport providers, or service providers.

Fraudulent requests may involve the purchase of seeds, fertilisers, pesticides, livestock, machinery, irrigation equipment, renewable energy systems, or other agricultural inputs. Criminals may also send false invoices or provide altered banking details.

Before making a payment, verify the supplier's identity, invoice details, delivery arrangements, and banking information through a trusted communication channel.

2.7 Business Email Compromise and Payment Fraud

Business Email Compromise (BEC) occurs when criminals gain access to legitimate email accounts or impersonate trusted individuals to manipulate financial transactions.

For example, a fraudster may pose as an Academy employee, supplier, funder, or business partner and request an urgent payment or announce a change in banking details.

These scams may involve intercepted correspondence, forged invoices, or messages that appear to come from senior management.

Always confirm payment instructions and changes to banking details verbally or through another independently verified channel before transferring money. Never rely solely on an email or message to authorise a financial transaction.

3. How to Protect Yourself and the Academy

The following practices can help reduce cybersecurity risks and protect personal, organisational, and agricultural information.

3.1 Verify Emails, Messages and Attachments

- Do not click on suspicious links or open unexpected attachments.
- Check email addresses, telephone numbers, website addresses, and social media account details carefully.
- Be cautious of messages that create urgency, threaten consequences, or promise benefits that seem too good to be true.
- Independently verify requests involving sensitive information, payments, funding applications, or changes to banking details.
- Report suspicious messages to the Academy through its designated official communication channels.

3.2 Use Strong and Unique Passwords

- Create long, unique passwords for each important account.
- Avoid using easily guessed information, such as names, birthdays, identity numbers, or farm names.
- Do not share passwords with colleagues, trainees, suppliers, or other individuals.
- Use a reputable password manager where practical.
- Change compromised passwords immediately and secure any other accounts that may use the same credentials.

3.3 Enable Multi-Factor Authentication

Where available, enable multi-factor authentication (MFA) for email, online banking, social media, cloud storage, and other important accounts.

MFA provides an additional layer of security by requiring another verification step in addition to a password. Use an authenticator application, security key, or other secure verification method where available.

Never share verification codes or approve login requests that you did not initiate.

3.4 Protect Social Media Accounts

- Use privacy settings to control who can view personal and professional information.
- Avoid publicly sharing identity documents, financial details, passwords, or confidential Academy information.
- Verify social media pages and accounts before relying on their announcements.
- Report suspicious profiles that impersonate the Academy or its representatives.
- Obtain appropriate authorisation before publishing photographs, personal information, or records relating to farmers, trainees, staff, and programme beneficiaries.

3.5 Limit the Sharing of Personal Information

Share personal and organisational information only when necessary and with authorised recipients.

Be particularly careful when providing identity documents, banking details, contact information, farm ownership records, funding applications, or beneficiary information.

Avoid posting sensitive details in public groups or sending confidential documents to unverified email addresses and messaging accounts.

3.6 Protect Important Data and Documents

Store important documents securely, including training records, farmer registration details, financial records, contracts, funding applications, and operational information.

- Restrict access to authorised individuals.
- Use encryption where available to protect sensitive files.

- Back up important data regularly using secure storage solutions.
- Keep backup copies separate from primary systems where practical.
- Dispose of confidential paper documents securely, including unnecessary bank statements, invoices, and identity document copies.

3.7 Secure Mobile Phones, Computers and Other Devices

Use a secure PIN, password, fingerprint, or facial recognition to protect devices.

Keep devices locked when unattended and avoid leaving them accessible to unauthorised individuals. Do not save passwords in unsecured locations or display sensitive information on lock screens.

When using shared computers at training venues, offices, community facilities, or internet cafés, avoid saving passwords and always sign out of accounts when finished.

3.8 Keep Software and Applications Updated

Install software and security updates as soon as reasonably possible. Keep operating systems, browsers, antivirus tools, and mobile applications up to date.

Where appropriate, enable automatic updates and use reputable security software.

Only install applications from trusted sources and remove applications that are no longer required.

3.9 Use Secure Internet Connections

Be cautious when using public Wi-Fi networks at airports, hotels, community centres, or other public locations.

Avoid accessing sensitive accounts or conducting financial transactions over unsecured public networks. Where possible, use a trusted mobile connection or an appropriately configured virtual private network (VPN).

At home, on farms, and in offices, protect Wi-Fi networks with strong passwords and up-to-date router security settings. Provide visitors with a separate guest network where practical.

3.10 Protect Agricultural and Business Records

Farmers and agricultural enterprises should take reasonable steps to protect digital records relating to production, livestock, customers, suppliers, financial transactions, farm operations, and agricultural technology.

Where digital systems are used to monitor irrigation, renewable energy, equipment, or other farm infrastructure, access should be restricted to authorised users. Default passwords should be changed, and connected devices should be secured and updated where possible.

These precautions help reduce the risk of unauthorised access, operational disruption, and the loss of valuable farming information.

4. Identity Theft and Personal Information Protection

Identity theft occurs when someone obtains and uses another person's personal information without permission, often to commit fraud or impersonate that person.

Stolen information may be used to open accounts, apply for credit, obtain services, submit fraudulent applications, or deceive other individuals and organisations.

To reduce the risk of identity theft:

- Do not share personal information with unfamiliar people, websites, or organisations.
- Verify the legitimacy of requests for identity documents and banking information.
- Store physical and digital documents securely.
- Shred or securely dispose of unwanted documents containing confidential information.
- Monitor financial accounts and promptly report suspicious transactions.
- Report suspected identity theft to the relevant financial institution and appropriate authorities.

Farmers, trainees, and programme beneficiaries should be particularly cautious when submitting personal documents in connection with training, employment, funding, or agricultural support programmes.

5. Fraud Prevention and Financial Security

Financial fraud can affect farmers, suppliers, employees, programme beneficiaries, and organisations of any size.

The Academy encourages all stakeholders to exercise caution when receiving requests for payments or financial information.

To reduce the risk of financial fraud:

- Verify all payment instructions independently before making a transfer.
- Confirm any changes to banking details directly with the relevant organisation or supplier using previously verified contact information.
- Be cautious of requests for urgent or confidential payments.
- Check invoices, quotations, purchase orders, and supplier details for inconsistencies.
- Never disclose online banking passwords, PINs, or one-time verification codes.
- Retain appropriate records of transactions and approved payments.
- Report suspected fraud as soon as possible.

No payment should be made solely on the basis of an unverified message, social media post, email, or telephone call.

6. Responsibilities of Staff, Farmers, Trainees and Partners

Everyone associated with the Nett-Zero Farmers Academy has a role to play in maintaining a safe digital environment.

Employees and management should protect confidential information, follow approved security procedures, use authorised systems, and report suspicious activities promptly.

Farmers and trainees should verify programme announcements, protect their personal information, and exercise caution when responding to messages about training, grants, employment, equipment, or financial assistance.

Suppliers and business partners should independently verify procurement requests, invoices, payment instructions, and changes to banking details before taking action.

All stakeholders should avoid forwarding unverified information, sharing confidential documents without authorisation, or allowing unauthorised individuals to access accounts and devices.

7. What to Do if You Suspect a Cyberattack or Fraud

If you suspect that you have received a fraudulent message, clicked on a malicious link, disclosed confidential information, or experienced unauthorised access to an account, take action as soon as possible.

1. **Stop communicating with the suspected fraudster.** Do not send further information or money.
2. **Secure your accounts.** From a trusted device, change compromised passwords and enable multi-factor authentication where possible.
3. **Contact your bank immediately** if banking details have been exposed or an unauthorised transaction has occurred. Request assistance in securing the account and stopping or recovering payments where possible.
4. **Protect affected devices.** Disconnect a device from the network if it appears compromised, and seek appropriate technical assistance.
5. **Preserve evidence.** Keep relevant emails, messages, telephone numbers, transaction records, screenshots, and website addresses.
6. **Notify the Nett-Zero Farmers Academy** through its designated official reporting channel if the incident involves the Academy, its staff, trainees, farmers, programmes, systems, or partners.
7. **Report the incident to the appropriate authorities** where necessary, particularly in cases involving financial fraud, identity theft, or unlawful access to information.

Prompt reporting can help limit financial losses, protect affected individuals, and prevent similar incidents from occurring.

8. Official Communications and Verification

Fraudsters may use the Academy's name, logo, photographs, or programme information without authorisation. The appearance of official branding does not, by itself, prove that a communication is genuine.

Before responding to an announcement or request relating to the Nett-Zero Farmers Academy:

- Confirm the information through the Academy's established official communication channels.
- Verify the identity of the person making the request.

- Confirm any registration fees, payment requirements, funding arrangements, or banking details independently.
- Do not rely exclusively on forwarded messages, unofficial social media pages, or personal accounts claiming to represent the Academy.

The Academy should communicate its official contact details, approved payment procedures, and designated fraud-reporting channel clearly to staff, farmers, trainees, suppliers, and partners.

To report a suspicious communication or suspected fraud involving the Nett-Zero Farmers Academy, please contact the Academy through its verified official communication channels. If you are unsure whether a communication is legitimate, verify it before responding or taking any action.

9. Conclusion

Cybersecurity and fraud prevention are shared responsibilities. As agriculture increasingly adopts digital technologies and online communication, protecting information, financial resources, farming operations, and stakeholder trust becomes essential.

The Nett-Zero Farmers Academy encourages all employees, farmers, trainees, suppliers, partners, and other stakeholders to remain alert, verify suspicious communications, protect confidential information, and report potential cyber threats promptly.

By adopting responsible digital practices and working together, we can create a safer and more trustworthy environment that supports agricultural development, farmer empowerment, sustainable farming, and the Academy's commitment to a net-zero future.