Fraud Awareness and Prevention

Training for Trustees and Volunteers

ANTHONY NOLAN

ANTHONY NOLAN

Course Content

- What is fraud?
- What is internal fraud?
- What is external fraud?
- The consequences of fraud
- Reporting suspicious activity
- Policies and further reading

ANTHONY NOLAN

What is Fraud?

The Anthony Nolan Anti-Fraud Policy defines fraud as

'***a deliberate intent to acquire money or goods dishonestly* through the falsification of records or documents'**

Examples of fraud include:

* Theft of funds or other Anthony Nolan property;

* False accounting or any other falsification of costs, expenses, or financial records;

* Forgery or alteration of documents;

* Destruction or removal of records;

* Inappropriate use of Anthony Nolan property;

* Seeking or accepting cash, gifts or other benefits from a third party in exchange for preferment of the third party in their dealings with Anthony Nolan;

* Blackmail or extortion and;

*Cyber fraud, phishing and/or scamming activities such as the creation of fake email addresses or bank accounts.

Fraud can be committed for the benefit or to the detriment of the organisation by persons outside as well as inside Anthony Nolan. The attempt to deceive is a criminal act, and we treat attempted fraud as seriously as accomplished fraud.

ANTHONY NOLAN

Internal Fraud

Internal fraud is when employees, volunteers or service providers defraud their own organisation, suppliers or customers. Examples of how individuals may commit internal fraud include:

- Keeping monetary donations to themselves that were meant for the charity.
- Claiming false or inappropriate expenses.
- Abusing their position of trust or authority to override financial controls.
- Copying or downloading confidential data (eg lists of contacts) to use for themselves or sell on.

All employees and volunteers should be alert to suspicious **warning signs**, which may include:

- Missing documents
- Unusual transactions or unexplained discrepancies
- Colleagues displaying unusual or changed behaviour, or circumstances that may make them more prone to commit fraud.

Anthony Nolan have measures in place to help reduce the opportunity for fraud to happen. It is the responsibility of every employee or person working on our behalf to help prevent and identify fraud.

External Fraud

External fraud is when someone outside of the organisation gains access to the organisation to defraud or acquire data. Such breaches may occur when someone working for or on behalf of Anthony Nolan receives a fraudulent email that is designed to trick them into visiting a website, sending information or signing into an account.

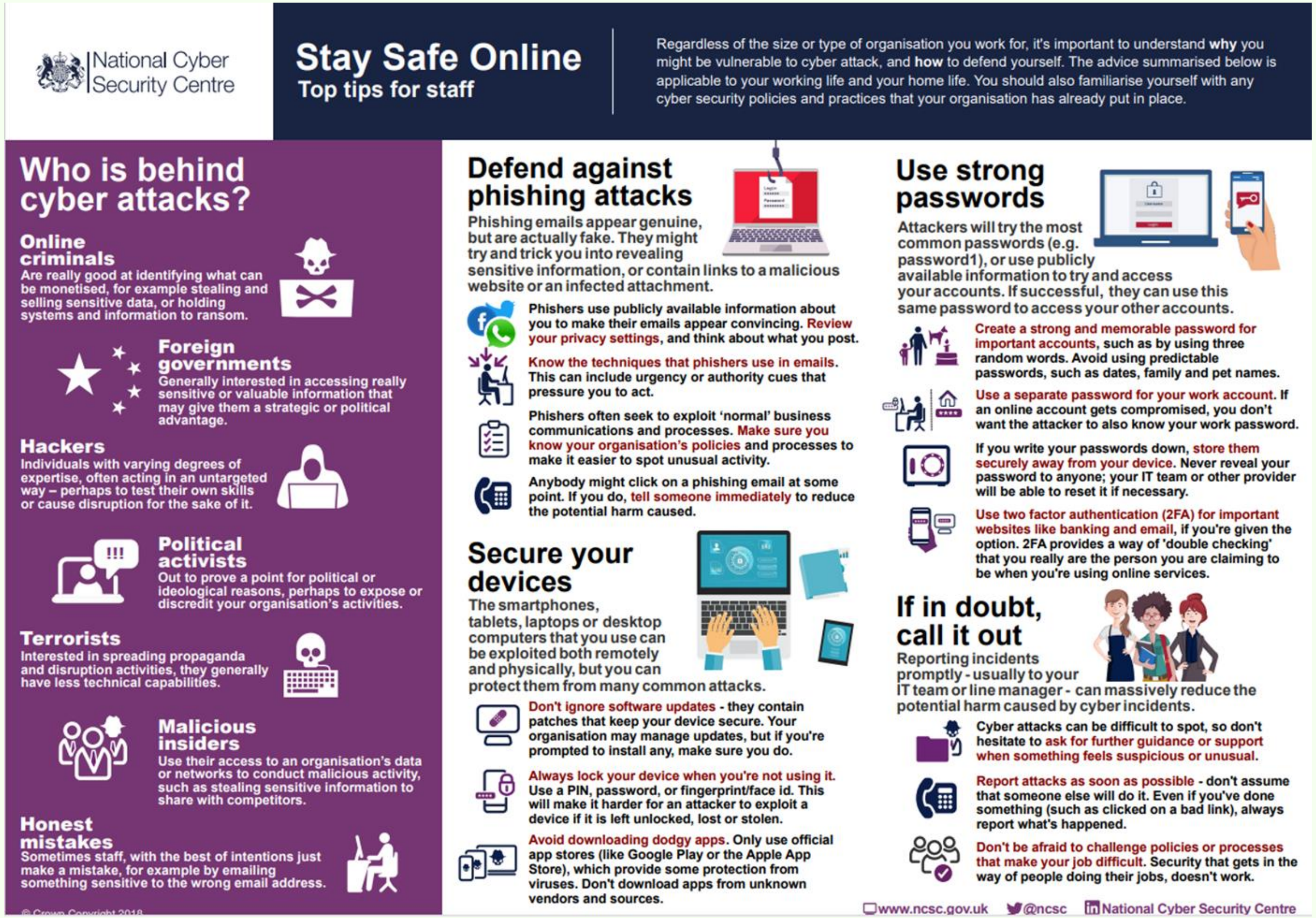
Employees and anyone working on behalf of Anthony Nolan are advised to remain cautious – do not answer or open anything that seems suspicious. Anyone using Anthony Nolan equipment should use the firewall and anti-virus software provided to protect against these kinds of threats.

Using a strong password is very important – it should be easy for you to remember but difficult for others to guess, and you should never use the same password repeatedly.

The National Cyber Security Centre provides some useful tips on staying safe online on the next page.

Any suspicions of fraud must be reported promptly to Anthony Nolan through your volunteer manager.

External Fraud



National Cyber Security Centre

Stay Safe Online

Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand **why** you might be vulnerable to cyber attack, and **how** to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals
Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Foreign governments
Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers
Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Political activists
Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists
Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.

Malicious insiders
Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes
Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.

Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.

Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.

Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.

Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.

Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.

If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.

Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

Consequences of Fraud

Fraud can have devastating consequences for charities, extending beyond financial losses. It can damage the charities reputation, erode public trust and lead to reduced fundraising and volunteering. This can potentially impact the charity's work and reduce the number of people it can serve.

Under the Economic Crime and Corporate Transparency Act 2023, from September 2025 Failure to Prevent Fraud is an offence for large organisations, including Anthony Nolan. The offence holds large organisations liable if an employee commits fraud that the organisation benefits from, regardless of whether the organisation is aware of the fraud.

There are serious consequences for perpetrators too – they could lose their job, face criminal prosecution, get a criminal record or even a jail sentence depending on the severity of the case.

It is important to report any signs or warnings you may see, and not get drawn into fraudulent activities, no matter the reasoning or pressures.

Reporting Suspicious Activity

- If you become aware of suspected fraud or irregularity, write down your concerns immediately. Make a note of all relevant details, such as what was said in phone or other conversations, the date, the time and the names of anyone involved. Report the matter immediately to your volunteer manager.

- Do not contact or discuss the matter with the suspected perpetrator.

- Do not discuss the case, your suspicions or allegations with anyone else, unless specifically asked to do so (for example, by those conducting an investigation).

- Do not attempt to personally conduct investigations or interviews.

The decision to report a suspicion can be difficult to take, not least because of the fear of reprisal from those responsible for the suspected fraud.

Anthony Nolan have a Whistleblowing Policy in place, to enable employees, volunteers and Trustees to raise genuine concerns about possible wrongdoing at the Charity, without fear of reprisal.

Policies and Further reading

Anthony Nolan policies and procedures:

Anthony Nolan Anti-Fraud Policy

Anthony Nolan Whistleblowing Policy

Volunteer Policy Hub

External resources:

Prevent Charity Fraud website offers information and guidance including:

Failure to Prevent Fraud offence

Fundraising Fraud

The Charity Commission offers guidance to Protect your charity from fraud

Barclays Bank offer guidance Fraud Protection and Cyber Threats