Training Course on Cyberfraud Prevention for Retirees

Professional Development Training Course Outline

Category	Pension and Retirement	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As technology becomes increasingly integrated into daily life, retirees are often targeted by cybercriminals who exploit their vulnerabilities. Cyberfraud can take many forms, including phishing scams, identity theft, and online fraud, all of which can have devastating financial and emotional consequences. Given that many retirees may not be as familiar with digital technology and online security, it's crucial to equip them with the knowledge and tools necessary to protect themselves against cyber threats. Training Course on Cyberfraud Prevention for Retirees aims to educate retirees about the various types of cyberfraud, how to recognize potential threats, and effective strategies to prevent becoming victims. Participants will learn about the importance of cybersecurity, safe online practices, and how to respond if they suspect they've been targeted. Through practical advice, real-world examples, and interactive discussions, this course will empower retirees to navigate the digital landscape confidently and securely. By the end of the course, participants will have a comprehensive understanding of cyberfraud prevention and the skills needed to protect their personal information and financial security in an increasingly digital world. This proactive approach to cybersecurity will help ensure that retirees can enjoy their online activities without fear.

Programme Curriculum

Training Course on Cyberfraud Prevention for Retirees

Introduction

As technology becomes increasingly integrated into daily life, retirees are often targeted by cybercriminals who exploit their vulnerabilities. Cyberfraud can take many forms, including phishing scams, identity theft, and online fraud, all of which can have devastating financial and emotional consequences. Given that many retirees may not be as familiar with digital technology and online security, it's crucial to equip them with the knowledge and

tools necessary to protect themselves against cyber threats.

Training Course on Cyberfraud Prevention for Retirees aims to educate retirees about the various types of cyberfraud, how to recognize potential threats, and effective strategies to prevent becoming victims. Participants will learn about the importance of cybersecurity, safe online practices, and how to respond if they suspect they've been targeted. Through practical advice, real-world examples, and interactive discussions, this course will empower retirees to navigate the digital landscape confidently and securely. By the end of the course, participants will have a comprehensive understanding of cyberfraud prevention and the skills needed to protect their personal information and financial security in an increasingly digital world. This proactive approach to cybersecurity will help ensure that retirees can enjoy their online activities without fear.

Course Objectives

1. Understand the various types of cyberfraud targeting retirees.
2. Recognize common signs of phishing and other scams.
3. Explore the importance of strong passwords and secure accounts.
4. Discuss safe online practices for browsing and shopping.
5. Identify the role of technology in protecting against cyber threats.
6. Analyze the implications of identity theft and how to prevent it.
7. Learn how to report cyber fraud and seek help.
8. Explore the importance of social media privacy settings.
9. Discuss the risks associated with public Wi-Fi networks.
10. Identify common scams specifically targeting older adults.
11. Learn about cybersecurity tools and software.
12. Develop a personal action plan for ongoing cyber safety.
13. Strategies for safeguarding personal information.

Target Audience

1. Retirees and individuals approaching retirement.
2. Family members and caregivers of older adults.
3. Community organizations focused on senior services.
4. Financial advisors and planners.
5. Healthcare professionals working with older populations.
6. Nonprofit organizations addressing aging issues.
7. Academics and researchers in cybersecurity.
8. Anyone interested in enhancing cyber safety for older adults.

Course Duration: 10 Days

Course Modules

Module 1: Introduction to Cyberfraud

- Define cyberfraud and its prevalence among retirees.
- Discuss the impact of cyberfraud on individuals and families.
- Explore the motivations behind cybercrime.
- Identify common terminology related to cyberfraud.
- Review statistics on cybercrime affecting older adults.

Module 2: Types of Cyberfraud

- Discuss common types of cyberfraud (phishing, identity theft, scams).
- Explore examples of each type of fraud targeting retirees.
- Analyze the tactics used by cybercriminals.
- Identify red flags that may indicate a fraudulent attempt.
- Review case studies of cyberfraud incidents.

Module 3: Recognizing Phishing Scams

- Define phishing and its various forms (email, phone, text).
- Discuss how to recognize phishing attempts.
- Explore the importance of scrutinizing URLs and email addresses.
- Identify common phrases and tactics used in phishing messages.
- Review case studies of phishing scams targeting retirees.

Module 4: Password Security and Account Protection

- Discuss the importance of strong passwords.
- Explore best practices for creating and managing passwords.
- Identify tools for password management (password managers).
- Analyze the role of two-factor authentication.
- Review case studies on account breaches due to weak passwords.

Module 5: Safe Online Practices

- Discuss safe browsing habits and online shopping tips.
- Explore the importance of secure websites (HTTPS).
- Identify how to avoid sharing personal information unnecessarily.
- Analyze the risks of clicking on unknown links or attachments.
- Review case studies of safe online behavior.

Module 6: Protecting Personal Information

- Discuss the implications of identity theft for retirees.
- Explore strategies for safeguarding personal information.
- Identify what information should be kept private.
- Analyze the role of social media in identity theft.
- Review case studies of identity theft incidents.

Module 7: Reporting Cyber Fraud

- Discuss the steps to take if one suspects fraud.
- Explore how to report cyber fraud to authorities.
- Identify resources for assistance (local law enforcement, FTC).
- Analyze the importance of sharing experiences to raise awareness.
- Review case studies of successful fraud reporting.

Module 8: Social Media Safety

- Discuss the risks associated with social media use.
- Explore privacy settings and how to adjust them.
- Identify safe practices for sharing information online.
- Analyze the impact of oversharing on personal safety.

- Review case studies of social media-related scams.

Module 9: Risks of Public Wi-Fi Networks

- Discuss the dangers of using public Wi-Fi.
- Explore best practices for safe internet use in public spaces.
- Identify tools for securing connections (VPNs).
- Analyze real-world examples of public Wi-Fi exploitation.
- Review case studies of incidents involving public Wi-Fi.

Module 10: Common Scams Targeting Older Adults

- Discuss prevalent scams targeting retirees (lottery scams, tech support).
- Explore how to recognize and avoid these scams.
- Identify resources for checking scam alerts.
- Analyze the psychological tactics used in these scams.
- Review case studies of victims of common scams.

Module 11: Cybersecurity Tools and Software

- Discuss essential cybersecurity tools (antivirus, firewalls).
- Explore software options for protecting devices.
- Identify apps for secure online banking and shopping.
- Analyze the importance of keeping software updated.
- Review case studies of effective tool use in cybersecurity

Module 12: Developing a Personal Action Plan

- Discuss the importance of ongoing cyber safety education.
- Explore steps for creating a personal cybersecurity action plan.
- Identify resources for continued learning about cyber safety.
- Analyze how to regularly assess and update security measures.
- Create a personal action plan for ongoing vigilance against cyberfraud.

Training Methodology

- **Interactive Workshops:** Facilitated discussions, group exercises, and problem-solving activities.
- **Case Studies:** Real-world examples to illustrate successful community-based surveillance practices.
- **Role-Playing and Simulations:** Practice engaging communities in surveillance activities.
- **Expert Presentations:** Insights from experienced public health professionals and community leaders.
- **Group Projects:** Collaborative development of community surveillance plans.
- **Action Planning:** Development of personalized action plans for implementing community-based surveillance.
- **Digital Tools and Resources:** Utilization of online platforms for collaboration and learning.
- **Peer-to-Peer Learning:** Sharing experiences and insights on community engagement.
- **Post-Training Support:** Access to online forums, mentorship, and continued learning resources.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

- Participants must be conversant in English.
- Upon completion of training, participants will receive an Authorized Training Certificate.
- The course duration is flexible and can be modified to fit any number of days.
- Course fee includes facilitation, training materials, 2 coffee breaks, buffet lunch, and a Certificate upon successful completion.
- One-year post-training support, consultation, and coaching provided after the course.
- Payment should be made at least a week before the training commencement to Fineskill Training Center account, as indicated in the invoice, to enable better preparation.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com