19/03/2023

A Guide to Supporting Cyber Awareness

Phoenix

YOUTH PROVISION

Robin Sutton

❖ Contents

❖ Introduction

It is understandable to have a fear of being scammed online, as there are many potential risks and threats. However, it is possible to take steps to alleviate this fear and for everyone to feel more confident and secure when using the internet. The key is to be proactive and provide communities with the information, resources, and confidence they need to protect themselves.

If people are feeling overwhelmed or anxious about online scams, our role as ambassadors is to reach out and become a trusted friend who can offer the support they need.

❖ What Do People Need to Know?

To avoid being scammed, people need to be aware of the following information:

Common Scams

People need to understand common types of scams, such as phishing emails, fake websites, online shopping scams, romance scams, and investment scams.

Warning Signs

People need to be able to recognize warning signs of scams, such as unsolicited emails, phone calls, or messages; requests for personal information, especially financial information; pressure to act quickly; and promises of large rewards or returns.

Personal Information Protection

People need to know how to protect their personal information, such as using strong passwords, avoiding public Wi-Fi networks, and being cautious about giving out personal information online or over the phone.

Verification

People need to verify the legitimacy of any requests or offers that they receive, such as by checking the company's website or contacting them directly.

Secure Payment Methods

People need to know about secure payment methods, such as credit cards or payment services like PayPal, and avoid sending money through wire transfers, gift cards, or cryptocurrencies, which are commonly used in scams.

Keeping Software Up to Date

People need to keep their software, especially their antivirus and security software, up to date to prevent attacks from malware or viruses.

Reporting Scams

People need to know how to report scams to relevant authorities, such as Action Fraud, their bank, or the police.

By being aware of these essential pieces of information, people can protect themselves from being scammed and avoid falling victim to fraudulent activities.

❖ Learning About Online Fraud

Helping people learn about online fraud can involve several different approaches, but here are some ideas:

Share Resources

One of the best ways to help people learn about online fraud is to share reliable resources with them. This could include articles, videos, or infographics that explain common types of online fraud, how to recognize scams, and steps they can take to protect themselves.

Educate on Warning Signs

Make people aware of some of the most common warning signs of online fraud, such as requests for personal information, unsolicited emails or messages, or pressure to act quickly.

Emphasize Security Measures

Encourage people to take security measures to protect themselves, such as using strong passwords, two-factor authentication, and regularly updating their devices and software.

Discuss the Risks

Help people understand the risks of online fraud, both financial and otherwise, and the potential consequences of falling victim to scams.

Raise Awareness

Use social media or other platforms to raise awareness about online fraud, share stories of people who have been impacted by scams, and encourage others to stay vigilant and informed.

❖ Sharing Resources

Sharing resources about scams is an essential step in helping people protect themselves from fraud. Here are some ways to share resources about scams:

Social Media

Social media platforms like Facebook, Twitter, and LinkedIn are great places to share resources about scams. You can post links to articles, videos, and infographics, and encourage your followers to share them with their networks.

Email

Sending emails to friends and family with links to resources and information about scams is another effective way to share information. You can also encourage recipients to forward the emails to others they think might benefit from the information.

Websites and Blogs

If you have a website or blog, you can create a dedicated page or post with resources and information about scams. This can include links to articles, videos, and infographics, as well as tips and advice for staying safe online.

Community Groups

Community groups like Neighbourhood Watch schemes, religious organizations, and local clubs are great places to share information about scams. You can give presentations, distribute flyers or brochures, or host information sessions to help educate people about scams and how to avoid them.

Government Agencies

Government agencies like Action Fraud and Trading Standards have extensive resources about scams and can provide materials to share with your networks.

> *Remember, it's essential to share resources about scams in a way that is accessible and easy to understand. You can use plain language, visuals, and real-world examples to help people recognize and avoid scams. By sharing resources about scams, you can help protect others from falling victim to fraudulent activities.*

❖ Warning Signs

Scammers are becoming increasingly sophisticated, making it more challenging to identify their schemes. However, there are some common signs that can help you recognize scams. Here are some tips:

Unsolicited Communication

If you receive a call, text, email, or any other type of communication from someone you do not know or did not expect, be cautious. Scammers often contact potential victims out of the blue.

Requests for Personal Information

Scammers often ask for personal information such as your name, address, social security number, or financial information. Be suspicious of any requests for personal information that come from an unknown source.

Pressure to Act Quickly

Scammers will often try to create a sense of urgency to push you into making a hasty decision. Be wary of anyone who pressures you to act quickly without giving you time to think it over or do research.

Too Good to be True Offers

Scammers often promise you unrealistic rewards, like winning a lottery or a huge cash prize, or promise a large return on investment for a small amount of money.

Poor Spelling and Grammar

Many scammers use poor spelling and grammar in their messages, emails, and websites. This is because many scammers operate from countries where English is not the primary language.

The Sense of Trust

Scammers may try to gain your trust by using official-looking logos, email addresses, or websites that seem legitimate but aren't. They may also pretend to be from a company or organization you trust.

Payment Requests

Scammers often ask for payment in unusual ways, such as through wire transfers, gift cards, or cryptocurrencies. Be cautious of any requests for payment that are outside the norm.

> *It's essential to stay vigilant and trust your instinct when it comes to identifying scams. If something feels off or too good to be true, it's best to do your research and verify the information before taking any action.*

❖ What Security Measures Should I Take?

There are several security measures that you can take to avoid being scammed.

Keep Your Personal Information Safe.

Be cautious about sharing your personal information online, including your full name, home address, phone number, and email address. Use strong, unique passwords for each account, and consider using a password manager to keep track of them.

Be Cautious of Unsolicited Emails or Phone Calls

Scammers often use unsolicited emails or phone calls to try to trick you into giving away personal information or money. If you receive an unsolicited email or phone call, be suspicious and do not give out any personal information until you can verify the legitimacy of the request.

Verify Requests for Personal or Financial Information

If you receive a request for personal or financial information, verify the request before providing any information. Contact the organization or person directly using a phone number or email address you know to be legitimate and confirm the request before providing any information.

Use Secure Payment Methods

Use secure payment methods, such as credit cards, that offer protection against fraudulent transactions. Avoid using payment methods that are difficult to trace or refund, such as wire transfers or prepaid debit cards.

Keep Your Software Up to Date

Keep your computer's operating system, internet browser, and security software up to date to protect against known security vulnerabilities.

Use Two-Factor Authentication

Two-factor authentication adds an extra layer of security by requiring a second form of verification, such as a text message or fingerprint scan, before allowing access to an account.

Be Cautious When Using Public Wi-Fi:

Public Wi-Fi networks are often not secure, and hackers can intercept data transmitted over these networks. Avoid accessing sensitive information, such as banking or credit card information, while connected to public Wi-Fi.

> *By following these security measures, you can help protect yourself against scammers and avoid falling victim to fraudulent activities.*

❖ What are the Risks?

Being scammed can lead to a variety of risks and negative consequences, including:

Financial Loss

Scammers often try to trick people into sending them money or providing access to their financial accounts. Victims of scams may lose significant amounts of money, which can lead to financial difficulties and even bankruptcy.

Identity Theft

Scammers may use stolen personal information to open new credit accounts or apply for loans, leading to identity theft and damage to credit scores.

Emotional Distress

Falling victim to a scam can cause emotional distress, including feelings of betrayal, anger, and embarrassment.

Compromised Security

Scammers may trick people into downloading malicious software or providing access to their devices, compromising their security and potentially allowing hackers to access sensitive information.

Legal issues

In some cases, victims of scams may face legal issues, such as being held responsible for fraudulent transactions or facing criminal charges if they unknowingly participate in illegal activities.

Reputation Damage

Victims of scams may suffer damage to their personal or professional reputations, particularly if their personal information is used to perpetrate a scam.

> *Overall, being scammed can have significant negative consequences, both financial and emotional. It is important to take steps to protect yourself against scams and to be vigilant in identifying and avoiding potential fraud.*

❖ Sharing Scam Resources

Sharing resources about scams is an important way to help others stay safe online. Here are some steps to follow when sharing resources about scams:

Identify the Resources

Find reliable resources about scams from reputable sources such as government agencies, consumer protection organizations, or financial institutions. These resources can include articles, videos, infographics, or tip sheets.

Choose Your Platform

Decide where you want to share the resources, such as social media, email, a website, or a community group. Consider the audience and the best way to reach them.

Customize Your Message

Craft a clear and concise message that explains why the resource is important and how it can help the reader. Use plain language and avoid technical jargon.

Share the resource:

Share the resource using the platform you have chosen. If you are sharing on social media, include relevant hashtags to increase visibility. If you are sharing via email, personalize the message and explain why you think the recipient would find it useful.

Encourage Engagement

Encourage your audience to engage with the resource by asking for feedback, comments, or questions. This can help foster discussion and encourage others to share the resource with their networks.

Monitor Engagement

Monitor the engagement with the resources and respond to any questions or comments. This can help build trust and establish you as a reliable source of information.

> *Remember, sharing resources about scams is an ongoing process. Stay up to date with the latest information and continue to share resources with your networks to help others stay safe online.*