SECURITY MATTERS
NEWSLETTER

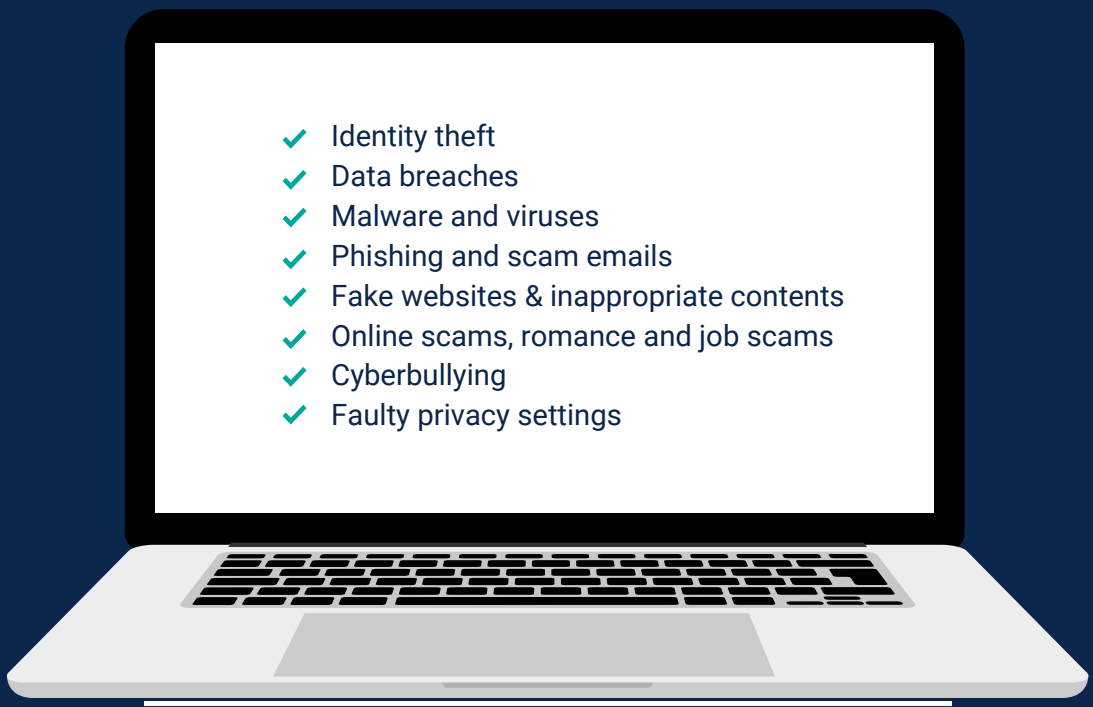
KEEP YOUR FAMILY SAFE ONLINE: TIPS AND TRICKS

VOL 9 • FEBRUARY 2023

Every day, we have the opportunity for online integration, and most of us own multiple devices, including laptops, phones, tablets, smart watches, smart TVs and more. The more accounts and devices we have online, the greater potential for criminals to access our personal information and take advantage of us.

Internet safety is important regardless of age or life stage, but there are particular concerns for certain vulnerable groups like children, teenagers and the elderly. Children learn how to operate a touchscreen before they can talk, and teens have access to various games and educational materials at their fingertips. Scammers take advantage of the elderly because many of them have a lifetime's worth of savings and other valuable assets. That's why it's essential to understand internet safety rules that protect us and our family from threats. Read on to find out about safer internet tips to avoid them.

We expose ourselves to a range of potential online threats daily, such as:



General Helpline: help@securitymatters.asia
Secure Communication via Protonmail:
secmhelpdesk@pm.me

More information about Security Matters,
visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

SECURITY MATTERS
NEWSLETTER

KEEP YOUR FAMILY SAFE ONLINE: TIPS AND TRICKS

VOL 9 • FEBRUARY 2023

SAFER INTERNET TIPS FOR CHILDREN & TEENS

1. Set clear online rules for children and teens to follow, including creating lists of approved websites and applications.
2. Limit online times.
3. Switch on parental and privacy controls.
4. Enable "Safe search" features for filtering objectionable content.
5. Limit technology use. Use an app like "Apple's Screen Time" to monitor and restrict device usage. Similar apps exist for Android devices.
6. Keep track of their online activity and friends, encourage them to avoid talking to strangers online.
7. Educate children and teens about online safety.
8. Do not show your face or leak anything personal.
9. Keep information private. Do not share passwords to others.
10. Never go to unknown websites. Block bullies.
11. Always be cautious of app location settings.
12. Create a safe space for conversations. Encourage children and teens to talk to a trusted adult if they're unsure about something they find on the internet.

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

SECURITY MATTERS
NEWSLETTER

KEEP YOUR FAMILY SAFE ONLINE: TIPS AND TRICKS

VOL 9 • FEBRUARY 2023

SAFER INTERNET TIPS FOR THE ELDERLY

1. Build trust with your parents/elderly.
2. Keep privacy settings on. Ensure you understand the privacy policy.
3. Educate elderly about basic online safety and common scams. Helps monitor their email accounts to keep an eye out for these threats.
4. Verify and think carefully before clicking on links and attachments in emails/text messages.
5. Be mindful of what is being shared on social media.
6. Ignore unsolicited phone calls and "robocalls".
7. Do not respond to or click on pop-up windows on devices.
8. Always validate someone's identity before trusting him/her, especially when being asked to send/receive money.
9. Never respond to something seems too good to be true.
10. Shop online only from secure sites.
11. When in doubt, ask family members or a trusted friend.

BASIC TIPS FOR ALL

1. Protect all devices with strong passwords. Enable two-factor or multi-factor authentication (2FA/MFA).
2. Beware of what you shared online.
3. Review apps and privacy settings and understand the policies.
4. Keep your device's software updated.
5. Backup files and data regularly.
6. Install anti-virus and anti-malware software.
7. Ensure your internet connection is secure.
8. Turn off Bluetooth when it's not in use.
9. Avoid using public WiFi to access personal information. Use a Virtual Private Network (VPN) if you have to.
10. Ensure the website you visited is reliable. Only log into sites that start with https://
11. Beware of phishing/scams. Discuss what phishing attempts are and how to identify them. Think and verify before clicking any links and attachments.
12. Delete unused accounts.
13. Beware on all online transactions.

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Related News

How to safely use payment apps

Scams are common on peer-to-peer payment apps, but you can keep your money safe by avoiding questionable payment requests that may be fraudulent, only sending money to people you know and upgrading your privacy settings. While payment apps are convenient, they also carry risks if you use them without first vetting who exactly you are sending money to. Fraud prevention experts recommend these strategies to keep your money safe.
Read more: http://bit.ly/40n7zEd

Denial-of-service attacks rise, raising concerns for banks

DDoS attackers marshal an army of connected devices (known as a botnet) and direct Internet traffic at a website to disrupt it or shut it down. As the attacks have gotten more powerful and easier for non-technical bad actors to execute, these are growing problem for banks and other financial businesses, according to a new report.
Read more: https://bit.ly/3YcI1rG

WhatsApp revamps status updates with new features

WhatsApp has once again introduced a set of new features to the app, this time focusing on revamping the experience for status updates. The new features will allow users to customise the privacy of their status, interact with them more easily, provide more mediums to update their status, and more.
Read more: http://bit.ly/3YBntJv

Meta's new ad policy further protects teen privacy and tackles discrimination

Teens will be able to – sort of – control what ads they see as Meta is updating the way it delivers advertisements to users in order to foster a more positive experience. The changes can be divided into two parts: one will restrict how companies that target teenage users while the other aims to make things more “equitable” and less discriminatory.
Read more:https://bit.ly/3CFqbVW

Bounty of browsers: How to choose the one that best fits your needs

While browsers for the most part do the same thing, there are a lot of aspects to consider besides how well they browse the Internet. The feature set on offer is a big part of what power users consider when picking their browser of choice.
Read more: http://bit.ly/3E1Opu6

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Alexa, who is listening?

Your smart speaker is designed to listen, but could it be eavesdropping too? There are lots of listening devices on the market, but those hiding in plain sight (and not normally thought of as 'listening bugs') are often the most commonly used. People don't normally realize how easily the devices themselves could be used as spying tools by anyone (more precisely, the device's admin) with illicit intent.
Read more: http://bit.ly/3xgu3th

Thai activists to sue government over Pegasus spyware use

Activists in Thailand are suing the government for using spyware technology to monitor dissidents, the first such case in the country that they hope will help raise awareness and better protect citizens who are subject to increasing surveillance. Legal non-profit iLaw told Context it is preparing a lawsuit against the Thai government for its alleged use of Israeli firm NSO Group's Pegasus spyware to hack into the mobile phones of at least 30 activists and lawyers in 2020-21.
Read more: http://bit.ly/3xGfFe6

Job scams are surprisingly smart. Here's how to not get burned

Today's scam ads are often indiscernible from legitimate listings, and can appear on reputable job sites like LinkedIn and Indeed, as well as in your inbox as phishing attacks. Most were click-and-go crimes, involving the minimum interaction to procure identity information or install malware. Today's scams are surprisingly elaborate, with fake company websites and phone or video interviews.
Read more: http://bit.ly/3RYzQNA

Personal data from 3 million MySejahtera users were downloaded without authorization

Personal data from three million MySejahtera users have been downloaded without authorization back in 2021. The incident took place in 2021 but were only revealed to the public today. The unauthorized download was made by a single MyVAS Admin account that has been provided with a Super Admin access level.
Read more: http://bit.ly/3Se2Pxc

Fake installers targeting Southeast and East Asia

Experts has found a malware campaign that had been targeting Chinese-speaking people in Southeast and East Asia.by buying misleading advertisements to appear in Google search results that lead to downloading trojanized installers.The attackers created fake websites that look identical to popular applications such as Google Chrome, Firefox, WhatsApp, or Telegram, but in addition to providing the legitimate software that grants the attacker control of the victimized computer.
Read more: http://bit.ly/3YLexBM

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters