Pointing Out Cyber Crimes, Beginning with the Peace Sign

As if there weren't enough identity fraud to worry about already, technologists warn that today's cell phone cameras can capture a fingerprint accurately enough for someone to steal it.

You'd better re-think all those selfies flashing the peace sign, they warn, because while it's easy to change a password it's nearly impossible to alter a fingerprint.

Researchers React to Safety Threats

Japanese Professor Isao Echizen of the Digital Content and Media Sciences research division says he obtained fingerprints from photos of fingers taken from about 9 or 10 feet away, according to CNET's Luke Lancaster. Echizen warns against the popular peace sign specifically, noting that it's a rampant

trend in Japanese selfies. He says it easily allows would-be identity thieves to pair fingerprints and faces.

Obtaining biometric data from images has been an increasing risk in recent years, Planet Biometrics notes, with the German celebrity hacker Starbug, for example, lifting German Chancellor Angela Merkel's iris data from a public image.

Echizen's team at the National Institute of Informatics has developed a fingerprint anti-theft prevention technology, yet flashing peace signs in photographs remains common in Asia. "As camera resolution gets higher, it's becoming possible to image smaller things like a fingerprint or an iris," Echizen told Reuters.

Unfortunately, cyber fraud goes far beyond fraudsters harvesting fingerprint data from online selfies. The U.S. government says scam artists here and around the world defraud millions of people each year by using the internet to trick victims into sending money or giving out personal information.

Types of Internet Fraud

Internet schemes target victims in many ways:

- **Internet auction fraud. Products are misrepresented for sale on Internet auction sites, or not delivered to the customer.**
- **Credit card fraud. Scammers fraudulently obtain money or property through the unauthorized use of a credit or debit card or credit number.**
- **Investment fraud. False claims can be used to solicit investments or loans, or providing for the purchase, use or trade of forged or counterfeit securities.**
- **Nigerian letter or '419' fraud. Named for the violation of Section 419 of the Nigerian Criminal Code, this ploy combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter,**

email or fax is received by the victim.

Online Safety and Security

Get Safe Online warns internet users about fraudsters and abusers and offers a wealth of information about how to protect yourself, your family, your bank account and your online devices:

1. **Choose, use and protect your passwords carefully. Use a different one for every online account in case one or more get hacked.**
2. **Look after your mobile devices. Don't leave them unattended in public places. Protect them with a PIN or passcode.**
3. **Ensure you always have internet security software loaded on computers. Use a similar app on your mobile devices, and keep both updated and switched on. Remember that smartphones and tablets can be compromised as easily as computers.**
4. **Don't assume that Wi-Fi hotspots in places like cafes, bars and hotel rooms are secure. Never use them when you're doing anything confidential online. Instead, use 3G or 4G or a VPN (virtual private network).**
5. **Never reveal too much personal or financial information in emails, on social networking and dating sites, or even in person. You never know who might see it, or use it.**
6. **Always consider that people aren't always who they claim to be. Fake emails and phone calls are a favorite way for fraudsters to approach their victims.**
7. **Don't click on links in emails, posts, tweets or texts – and don't open attachments – if the source isn't 100 percent known to you and trustworthy.**
8. **Never pay for anything by direct bank transfer – including goods, services, tickets, travel and holidays – unless it's to someone you know personally and is reputable.**
9. **Take your time and think twice. Everything may not be as**

it seems.

10. **Remember that if something seems too good to be true, it probably is.**

Reporting Cyber Crime

If you suspect you have been the victim of an internet crime, here are some actions you can take:

- **If you believe that someone is using your personal information, visit identitytheft.gov.**
- **The Internet Crime Complaint Center refers internet-related criminal complains to federal, state, local or international law enforcement.**
- **econsumer.gov accepts complains about online and related transactions with foreign companies.**
- **The Department of Justice helps you report your computer, internet-related, or intellectual property crime to the proper agency based on the scope of the crime.**
- **File a police report with your local law enforcement agency.**

Vigilance Pays

Identity fraud is growing at an alarming rate, so it pays for consumers to be cautious. That means curtailing the information you share on social media, ensuring your internet information is sent via secure connections, immediately spiking suspicious emails and changing your passwords frequently.

It's not much fun to think about the bad guys online. Still, taking time to ensure your security and that of your credit, bank accounts and investments ultimately means great peace of mind.

For more information visit
co-opcreditunions.org