F-Alert

Monthly threat updates from

F-Secure

June 2024

F-Secure

Summer F-Alert: sun, sea, and cyber security

Summer has finally arrived. It's a time when most of us are outdoors basking in the sun – but not even the mighty sun can deter online criminals from their exploits. In this F-Alert, our experts explore the latest security threats, and we discuss what you can do to protect yourself online this summer.

- WhatsApp imposter scams soar
- The UK bans weak passwords
- Deepfakes deceive in real-time
- Summer cyber survival toolkit
- Can technology be trusted?
- Rising crime, rising captures
- Passkeys: the end of passwords?

Joel Latto
Threat Advisor
Helsinki, Finland

expert tip

Report and block any suspicious senders on WhatsApp and never share your account details, passcodes, and verification codes with anyone.

“Beware of any unexpected or unusual requests for money.”

WhatsApp imposter scams soar

Warnings issued over steep rise in scams impersonating family and friends.

In recent years, imposter scams have gained popularity with online fraudsters out to profit from fear. In fact, nearly half of all frauds reported in the US last year were related to imposter scams – and it's a similar story throughout the rest of the world.

WhatsApp scam claims €850,000

With almost 3 billion active users worldwide, WhatsApp is a favorite platform for scammers. In Spain, authorities recently arrested a group of more than 100 criminals who ran a callous ‘family in need’ scam. “To trick their victims into sending money, the scammers impersonated family members who needed urgent financial help,” explains Joel Latto, Threat Advisor at F-Secure.

“The gang targeted 238 victims and were so convincing in their deception that, in many cases, they received multiple payments of €800 to €55,000 per transfer.”

A recurring trend

In the UK, Action Fraud has issued a warning about a new ‘group chat’ WhatsApp scam that has targeted hundreds of victims. “Using a fake display name and profile photo and possibly even using AI, the scammer calls the victim pretending to be a member of a group chat,” Latto explains.

“The scammer tells the victim that they will send them a one-time passcode to join an upcoming call and to share it with them. But the ‘passcode’ is in fact an access code that lets the scammer register the victim’s WhatsApp account to a new device and take it over. They then message the victim’s contacts asking for money.”

What you should do

“Beware of any unexpected or unusual requests for money, even if they come from what appears to be a friend or family member. Stop and take time to think – scammers rely on hasty decisions made in an emotional state. Instead, call the phone number that you have saved for them outside of WhatsApp to see if they verify the request,” Latto concludes.

The UK bans weak passwords

Smart device manufacturers are legally required to meet new security standards.

In a recent crackdown on online crime, a new UK law has been passed that bans weak default passwords – such as '123456', 'admin', 'qwerty', and the old classic: 'password' – for internet-connected devices.

Tom Gaffney, Director of Embedded Security at F-Secure, discusses the impact of this new legislation which shifts the responsibility of securing devices from the consumer to the manufacturer.

Championing consumer security

"Smartphones and tablets. Home security devices. Wi-Fi routers. What do these things have in common? Unfortunately for consumers, the answer has historically been weak default passwords," says Gaffney.

"It's been easy for criminals to exploit vulnerabilities and gain unauthorized access to devices when users don't change the default password. That's why manufacturers must step up – and these new regulations will make sure they do."

Tightening product security

The UK's new regulations specify that brands must give each device a unique password, provide a public point of contact to report any vulnerabilities, and clearly state the minimum length of time that devices will receive security updates.

"This is a great development in consumer security, but it's not just a box to tick and be done with. The cyber threat landscape is ever evolving and, as such, this legislation must be continuously updated too," continues Gaffney.

"It's also important to note that non-compliant devices can still be bought from international online marketplaces and used in the UK, so consumers should bear this in mind when making purchases."

Keeping your devices secure

To make the most of any new security measures implemented by manufacturers, make sure you regularly update your devices when software updates are available. Change default passwords for devices and ensure each one is strong and unique – a password generator can help with this.

Tom Gaffney
Director, Embedded Security
London, UK

expert tip

Take some time to learn about the security features of your current devices and make sure any new device purchases prioritize security and are compliant with these regulations.

"This is a great development in consumer security."

Amit Table
Researcher
Helsinki, Finland

expert tip

Only a small number of tools create real-time deepfakes – but this will change. This technology is used in many types of scams, so always be on alert when interacting with people online.

“Never let your guard down during calls.”

Deepfakes deceive in real-time

Scammers are now tricking victims with face swap software during live calls.

Today, deepfakes are infamous. Something that started as an amusing activity for the tech-savvy – creating funny videos such as this deepfake of Tom Cruise doing “industrial cleanup” – is now more widely available, easier to use, and becoming a serious threat to people in real-time.

“Typically used to modify human faces with other human faces, deepfakes make use of machine learning and artificial intelligence algorithms,” explains Amit Tambe, Researcher at F-Secure. “And this provides an excellent platform for exploitation.”

A cutting-edge boost

While impersonation scams are already a well-known tactic, deepfakes significantly advance these efforts. Add in the ability to produce deepfakes in real-time, and scammers are seemingly unstoppable.

“Real-time deepfakes are being used during live video calls with potential victims by replacing the scammer’s face with the faces of people close to the victim, such as their spouse or children,” continues Tambe. “Scammers will scare grandparents into sending money to their ‘grandchild’, create deepfake ‘job hunters’ to dupe tech companies, and many other scenarios.”

Evolving techniques

According to a recent investigation, a criminal group known as the ‘Yahoo Boys’ have been experimenting with real-time deepfakes to carry out romance scams – and they aren't shy about it.

These scammers often use a setup of two phones: one is used to call the victim with its rear camera pointed at the second phone, which faces the scammer using a face swapping app.

Protecting yourself

While it’s challenging to detect deepfakes, there are some steps that you can take. According to Tambe: “Never let your guard down during calls with strangers – look for how they’re blinking, their eyebrows, the way their head turns, reflections in glasses, and similar signs of a glitch in the matrix. For calls with friends and family, introduce code words that strangers won’t know or guess.”

Summer cyber survival toolkit

While many of us will choose to be outdoors enjoying the sun over the next few months, cyber crime unfortunately doesn't stop for the summer. Here are some tips to help you stay secure.

Don't forget the basics

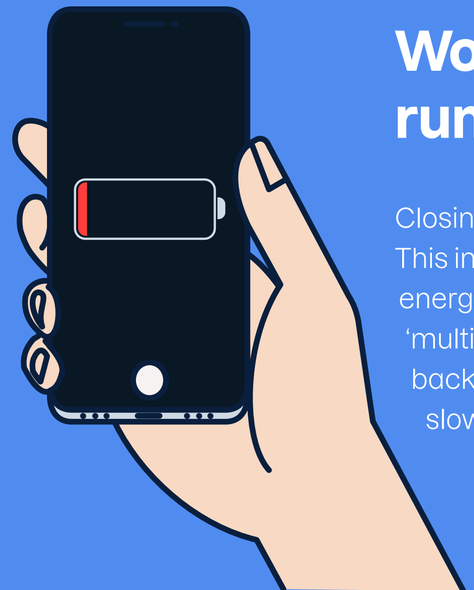
While screentime may reduce in the summer, it's important to remember cyber hygiene best practices:

1. Protect your devices with two-factor authentication and store unique passwords in a password manager.
2. Regularly update your software to ensure the latest security measures are in place.
3. Back up your devices to a cloud backup service such as OneDrive or iCloud.

Secure your devices from thieves

This year, Apple introduced Stolen Device Protection – a feature that fights back against theft or loss when away from familiar locations. We tested it and recommend that iPhone users enable it. Android will soon roll out a similar feature.

If you lose your device: try to track it using the 'Find My' service on another device and then lock your device using Android's Secure Device function or Apple's Lost Mode. Finally, report the loss to the relevant authorities and your mobile carrier.



Worried about your device running out of battery?

Closing background apps to save battery is a myth. This in fact worsens battery life as it requires more energy to load apps than to restart them from the 'multitasking' screen. These apps aren't running in the background, they're just suspended – so they won't slow your phone down either.

Going on vacation?

How to secure your digital moments

Before you leave

1

Take backups of devices and sync passwords from your password manager across multiple devices, so you won't lose access to services.

Time any smart lights to make it look like you're home and don't leave without giving your Wi-Fi and smart devices strong, unique passwords.

2

While on vacation

- **Use a VPN** when connecting to free public Wi-Fi while travelling.
- Make sure your device and SIM card are protected with a **strong PIN code and/or biometric authentication** in case your device is lost or stolen.
- **Disable airplane mode** for your SIM without a PIN code to make it more difficult for thieves to take the device offline and remote wipe.

3

Returning home

Check all the statements of any credit or bank cards used in person or online while on vacation.

Can technology be trusted?

A new report shows that our trust in tech innovations – like AI – is decreasing.

It's 2001. The iPod has hit the shelves. Microsoft has rolled out their latest operating system, Windows XP. Apple has just released Mac OS X. And for consumers, there's an air of excitement about the increasing digitalization of life.

More than two decades later in 2024, there's now a clear division between technological innovation and public trust. It's a paradox: consumers trust in technology companies, but not their innovations. And there's one innovation at the forefront of everyone's mind: artificial intelligence (AI).

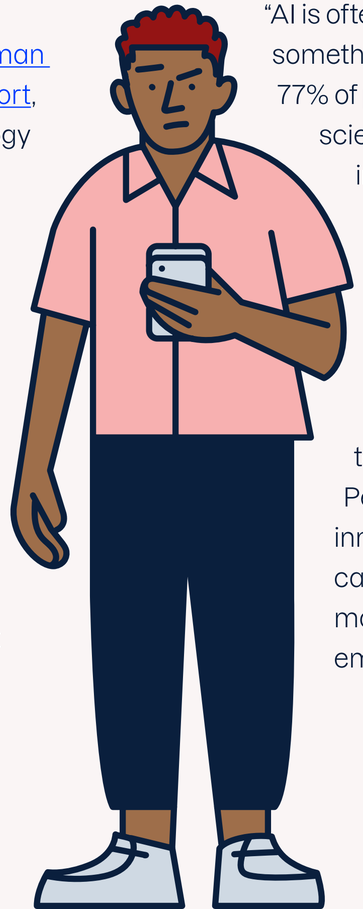
A state of distrust

"Tech companies have a wealth of opportunities to improve lives and make a positive impact on the planet thanks to rapid advancements in AI. However, the industry does have a blocking point: a lack of trust from the public," explains Timo Salmi, Senior Solution Marketing Manager at F-Secure.

"According to the 2024 Edelman Trust Barometer Global Report, 76% of people trust technology companies, but only 50% trust AI. Furthermore, only 30% of people embrace AI – while 35% reject it. So, while most people trust the industry, that doesn't necessarily mean that they trust its innovations."

Earning trust in AI

The root of the issue is a lack of understanding about AI globally – the language is complex, it's inaccessible and, in many cases, information comes from sources deemed untrustworthy by the public.



"AI is often described as something to fear. However, 77% of people say they trust scientists to lead on the implementation of innovation," continues Salmi. "So, it should be these experts who also explain the science and engage in dialogue with the public to help build trust in AI. People who understand innovations better and can see the benefits are most likely to accept and embrace them."

Timo Salmi
Senior Solution Marketing Manager
Oulu, Finland

expert tip

Take time to learn how AI is being used for good in the world, such as how Google is using it to accelerate climate action and the healthcare industry is using it to improve patient care.

"Only 30% of people embrace AI."

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

expert tip

If someone threatens you based on your breached private information, take it seriously. File a police report and remember that whatever is online can never be deleted – but it can be used as evidence.

“We always leave digital footprints behind.”

Rising crime, rising convictions

Online crime may be growing – but so is the number of criminals getting caught.

Last year, $1.026 trillion was stolen by scammers globally. Cyber crime is at an all-time high – but behind the scenes, cyber security specialists, police teams, and local authorities are diligently working to capture and convict online fraudsters, hackers, and criminal gangs.

Laura Kankaala, Head of Threat Intelligence at F-Secure, explores the outcomes of some recent cases.

Vastaamo case

“Last year, we reported on the Vastaamo Psychotherapy Center case, when a man was arrested for hacking, extortion, and leaking mental health records of over 30,000 patients,” says Kankaala.

“The scale of this crime is unprecedented – it's the biggest criminal case in Finnish history. And for Julius Kivimäki, judgement day has arrived: he has been sentenced to six years and three months in prison for crimes including aggravated data breach, aggravated extortion, and aggravated dissemination of information violating privacy.”

It took Finnish police almost two years to build a case against Kivimäki, using specialist digital forensics techniques such as extracting his fingerprint from a photo posted under an online pseudonym. According to Kankaala: “This case demonstrates that even though the internet and modern technology make it difficult to investigate crimes online, we always leave digital footprints behind.”

Operation Synergia

Another significant case to hit the news this year was Operation Synergia, led by INTERPOL. “Launched in response to growing transnational phishing, malware and ransomware threats, this operation was a coordinated action from 60 law enforcement agencies in more than 50 INTERPOL member countries,” explains Kankaala.

“During the operation, 1300 suspicious IP addresses or URLs were identified. 70% of the command-and-control (C2) servers have since been taken down, with the remaining under investigation, and authorities have arrested 31 individuals and identified 70 more suspects across the world.”

“This case demonstrates that the internet is not a bulletproof vest for scammers and criminals to use against law enforcement. When different authorities and online security experts work together, criminal infrastructures can be disrupted or dismantled entirely,” Kankaala concludes.

Passkeys: the end of passwords?

Google's plan to replace passwords with passkeys gets an anticipated update.

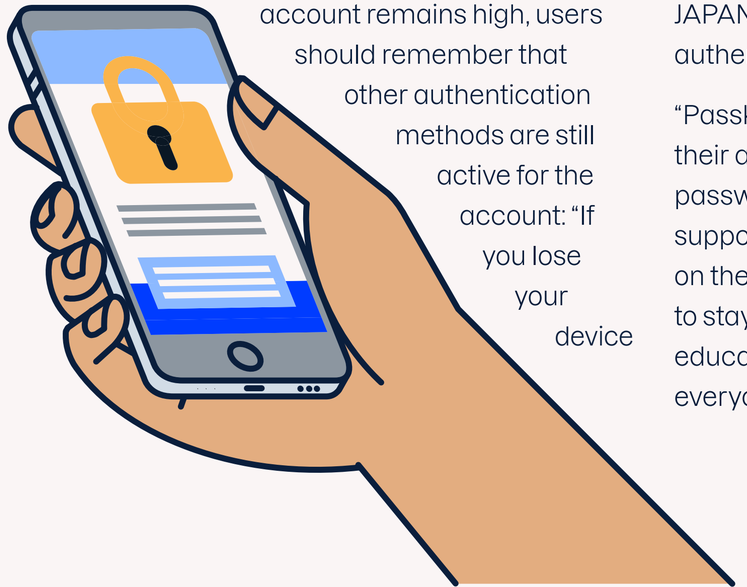
In 2022, Google launched passkeys: passwordless, device-based authentication that makes logging into your accounts quicker and more secure. The authenticator requires user verification – such as Face ID or Touch ID – to generate a passkey, which is then securely stored in a device's password manager.

A year later, passkeys were adopted in industry, and now two years since launch, more than 400 million Google accounts have used passkeys over 1 billion times. And from a recent update, it looks like momentum will only grow.

Lowering user risk

"While passwords can be guessed, hacked, stolen and bought on the dark web, passkeys are encrypted with no hackable data to exploit," explains Ash Shatrieh, Threat Intelligence Researcher at F-Secure. "Passkeys are replacing passwords for all the right reasons – if users adapt their daily life to using passkeys, they will automatically become more resistant to phishing attacks."

While the fear of losing trusted devices and not being able to log into an account remains high, users should remember that other authentication methods are still active for the account: "If you lose your device and, as a result, you also lose the passkey, you can still log in using your password," continues Shatrieh.



Growing industry support

Google's passkeys partner list has grown exponentially over the past year. The tech giant started with support from eBay, Uber, PayPal and Whatsapp, with Amazon, Docusign, Kayak, Mercari, Shopify and Yahoo! JAPAN later joining the passwordless authentication revolution.

"Passkeys are helping users sign into their accounts 50% faster than with passwords. This continued industry support suggests that passwords are on the way out and passkeys are here to stay – however, there's still some education to be done to convince everyone," Shatrieh concludes.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

While the move to replace passwords is in motion, it'll take years until it's commonplace. In the meantime, choose two-factor authentication when passkeys aren't an option, or use a password manager like F-Secure Total.

"Passkeys are encrypted with no hackable data."

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit f-secure.com today.

F-Secure