How to Prevent Phishing Scams: 5 Practical Tips

You opened the browser, logged in to your email, and realised an unread message sitting in your inbox. It goes like this:

"Dear Customer. We regret to inform you that your debit card account has been frozen. You need to urgently download the file attached to this email and update your login information."

What would you do in such a situation? Would you download the file or delete the phishy message and walk away? If you'd click, think twice next time before you click on any link in your email. Phishing attacks are avoidable, if been cautious enough. After reading this article, you'll learn how to prevent phishing scams with our 5 exclusive best practices.

5 Tips on How to Prevent Phishing Scams

Don't forget that you're a target of a phishing scam. If you understand how different types of phishing work, you'll surely know how to prevent phishing scams. Phishing scam prevention isn't a science but much more of an art and attentiveness.

1. Remain Informed About Common Phishing Attacks and Tactics

Can you recognize a phishing email? If not, then how you can prevent phishing scams? The best defence against phishing is remaining educated. Firstly, phishing can be conducted through text messages, social media, or by phone. But. the term phishing is majorly used to describe attacks that arrive by email. 96% of phishing attacks arrive via email. Phishing emails can hit an organization of any size and of any type. Be aware of different types of phishing attacks:

- **Vishing**: Voice phishing attack use advanced social engineering tactics to bait victims to reveal private information and access to bank accounts. The caller usually pretends to be calling from the tax department, police, the victim's bank or hospital. Vishing attacks can appear in different forms, such as unsolicited loan and investment offers, IRS tax scams, and social security scams. **To avoid a vishing attack, never provide your personal information on the phone. Also, pay attention to the language the**

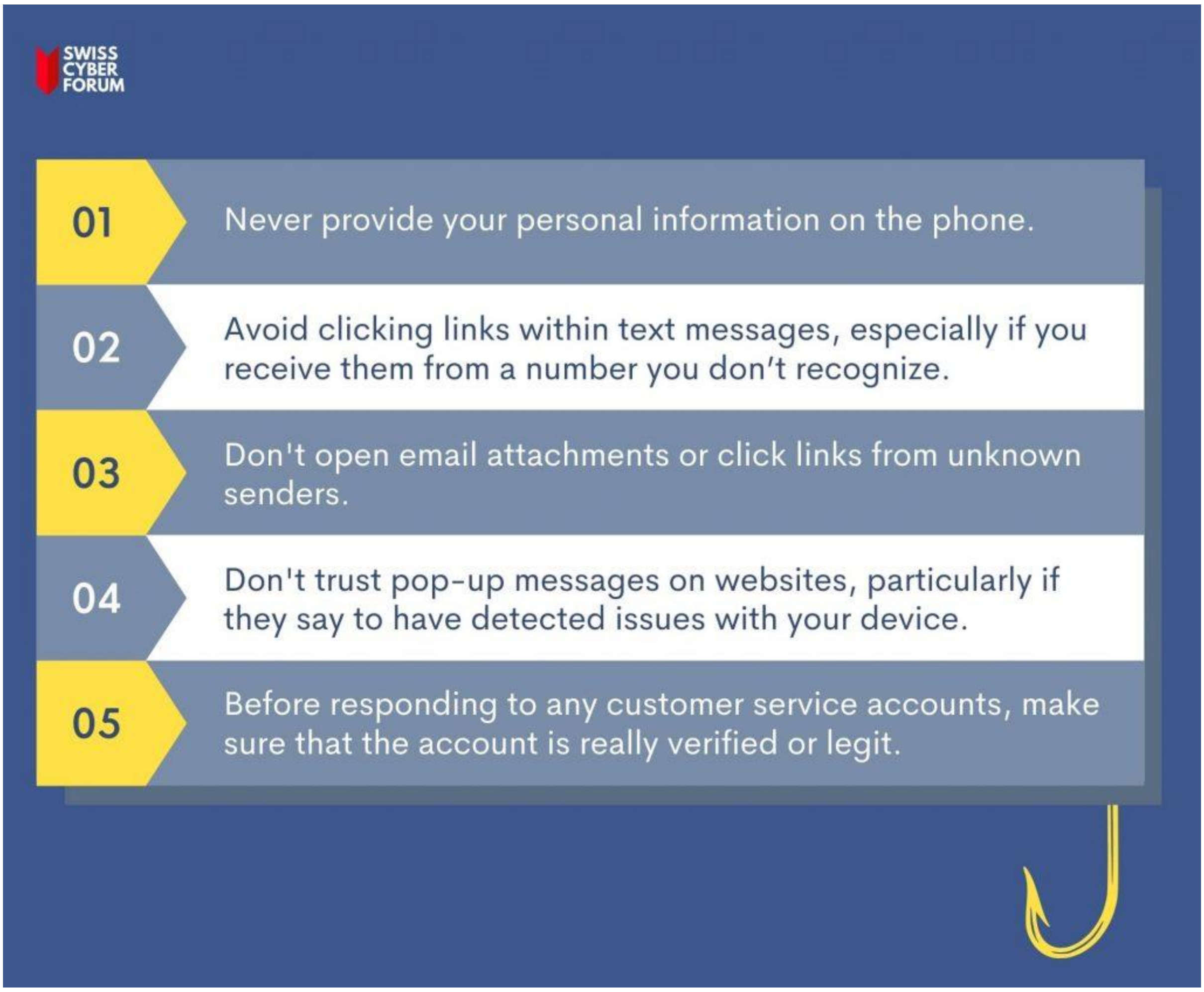
caller is using. In case you realize urgency or something mysterious, just hang up the phone.

- **Smishing**: This form of phishing attacks use mobile text messaging. Smihsing attacks are gaining popularity because people usually trust a message that comes in through a messaging app on their phone. Smishing attacks take on several forms. For example, you may receive fake survey links and notifications saying as if you've won a prize. We know that these tactics sound alluring, so the prevention of smishing attacks requires serious attention to detail. **The best practice here is to avoid clicking links within text messages, especially if you receive them from a number you don't recognize.**

- **Spear phishing**: Spear phishing attacks target specific individuals or groups within an organization. Did you know that spear phishing is the most widespread delivery method for advanced persistent threat (APT) attacks? A typical spear phishing attack has an email and attachment. The email includes information customized to the target, including the target's name and even position within the organization. Spear phishing attacks easily bypass traditional defenses because they use a combination of email spoofing, dynamic URLs and drive-by downloads. **To remain safe, don't open email attachments or click links from unknown senders.**

- **Pop-up phishing**: You are familiar with pop-ups that websites generate for more information. But, some of these pop-ups are harmful. Because fake pop-ups arre built to entice you into clicking on a button that redirects you to a fake website. The most famous fake pop-up usually displays "ransomware detected" message. Have you ever seen one? If yes, stay calm, it is probably a false security warning. **To avoid pop-up phishing attack, don't trust pop-up messages on websites, particularly if they say to have detected issues with your device.**

- **Angler phishing**: Angler phishing attacks are launched using fake corporate social media accounts. Fake accounts answer people who make their complaints on social media. Also, these accounts attempt to offer the dissatisfied person a link that they claim will take them to a support agent ready to talk to them. But in reality, clicking on that link will install malware onto your device. Do you want to know how to resist the lure? **Before responding to any customer service accounts, make sure that the account is really verified or legit.**


SWISS CYBER FORUM

01 Never provide your personal information on the phone.

02 Avoid clicking links within text messages, especially if you receive them from a number you don’t recognize.

03 Don't open email attachments or click links from unknown senders.

04 Don't trust pop-up messages on websites, particularly if they say to have detected issues with your device.

05 Before responding to any customer service accounts, make sure that the account is really verified or legit.

2. Keep All Your Applications Current With the Latest Security Patches

A security patch means a fix to a program that eliminates a vulnerability exploited by hackers. Applying security patches makes your device more secure. It may be annoying to interrupt your daily work, however, it’s 100% worth taking the time to download the latest software. You should install all the latest patches and updates to protect against vulnerabilities and security weaknesses. This includes website hosting, financial management software, personal finance platform, and content management software. We’re not only talking about updating apps and software but also mobile phones and operating systems.

Update later? Never again put off your device updates and reduce exposure to cyberattacks. To keep your operating system updated, follow the steps below:

- On Windows 10: **launch Start > Settings > Update & Security > Windows Update > to check for updates manually, select "Check for updates"**

- On Windows 8.1: **launch Start > Settings > Update and Recovery > Windows Update**

- On Windows 7: **please be informed that Microsoft has stapped supporting Windows 7 as of January 2020! It's seriously risky to use an operating system without security patches. Consider upgrading to Windows 8, 10 or 11.**

- On macOS: **from the Apple menu in the corner of your screen, choose System Preferences > Software Update > Update Now or Upgrade Now**

3. Install an Anti-phishing Extension or Add-on

Extensions are third-party programs that give your browser extra features and abilities. Anti-phishing extensions provide fast protection that is extensive across all of your devices. The beauty of these add-ons is that they give you a detailed report about the risk ratings on all the sites you visit recently. What can be more useful than these tools for those who aren't technologically savvy? You can download some of the well-known anti-phishing add-ons below (in order of the number of users).

- Avast Online Security (10,000,000+ users)

- Malwarebytes Browser Guard (8,000,000+ users)

- Microsoft Defender Browser Protection (1,000,000+ users)

- Bitdefender TrafficLight (700,000+ users)

- AVG Online Security (600,000+ users)

- Avira Safe Shopping (260,000+ users)

- Online Security Pro (80,000+ users)

- Netcraft (50,000+ users)

- TrustedSite (10,000+ users)

- PhishDetector (2,000+ users)

4. Treat Your Email Password Delicately

Do you treat your email passwords like you treat the keys to your home? No? But, you should. Your password is the key to your digital life. Cybercriminals don't just guess passwords. Instead, they use password cracking software that tries many combinations of letters and numbers. Although it sounds frustrating, there are ways to remain secure and prevent a phishing scam:

- **DON'T** include your first/middle/last names, the name of a close relative, your phone number, your license plate number into your password.
- **DON'T** click "yes" when asked to save your password to a particular browser.
- **DO** use a combination of uppercase and lowercase letters, symbols, characters, and numbers.
- **DO** make your passwords at least 12 characters long – the more complex, the better!
- **DO** log out of websites or devices when you finis using them.

5. Don't Click on Suspicious Links and Attachments

What do you do when you receive an attachment from an unknown sender? How cautiously do you behave? Cybercriminals send phishing emails with the hope of tricking victims into clicking links. A link is just a mechanism that delivers malware to your device. When you click on a suspicious link, you increase the risk of exposure to malware. Even a link that seems legitimate can infect your device.

The best practice here is to hover over the link to see the full URL. Then, you'll be able to tell whether the domain name matches that of the sender. Keep an eye on domains like **.work**, **.tw**, **.cn**, **.gq**, **.surf**, and **.ml**. As of October 2021, these are the domains with the worst reputations for spam operations.

Also, watch out for common company names but with misspellings or typos like **goigle.com**, **appel.com**, **insta-gram.com**, or **microsotf.com**. Typos, poor grammar and misspellings are direct red flag. Do you feel even a little suspicious? Walk away, don't click on anything and avoid a likely phishing scam.

Now You Know Better How to Prevent Phishing Scams

Phishing scams target people of all geographies, backgrounds, experiences and ages. Scams, unfortunately, succeed because they appear like the real thing. Although there is no single fool-proof way to prevent phishing attacks, you can still protect yourself. We encourage you to closely follow the 5 phishing scam prevention best practices we outlined above.

Don't rely on antivirus software and firewalls to stop cyberattacks. As a user or consumer, you need to use a combination of the technology stack and security best practices to protect your information assets. Check out our weekly blog posts and become savvier about cybersecurity. Continue with reading our previous articles: 5 Biggest Ransomware Attacks in History and How to Ensure Your Kids' Safety on the Internet.

Pasha Abdulov
Swiss Cyber Institute Cybersecurity Writer and Content Marketer