Internet Safety Guide

For content creators,
end-users & more

What You'll Learn

Here's what you'll learn in this **Internet Safety Guide**:

1. What to look for in your emails, such as **potentially malicious links, scams** and more.
2. An assortment of things to look for in comments as an **online content creator**.
3. **Popular content creator scams** and **regular scams** to be aware of.
4. Useful tips and tricks for implementing a **VPN**, **password management system** and more.
5. **Resources** from trusted sources.

Let's get started.

About Me

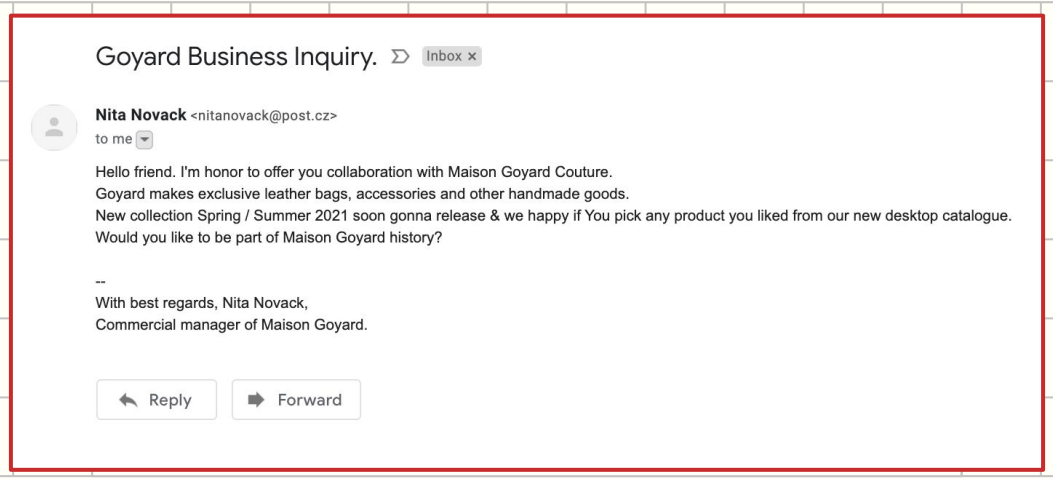
I work in ASMR, digital marketing and information security. I am advocate for tech equity and digital literacy with an emphasis content creator protection.

72%

of Americans believe their accounts are secure with only usernames and passwords, yet every two seconds there is another victim of identity fraud. Your usernames and passwords are not enough to keep your accounts secure.*

*(Stop. Think. Connect .(n.d.) "Lock Down Your Login", accessed 1-16-2017 from https://www.lockdownyourlogin.com).

What to Look For


Goyard Business Inquiry. Inbox ×

Nita Novack <nitanovack@post.cz>
to me

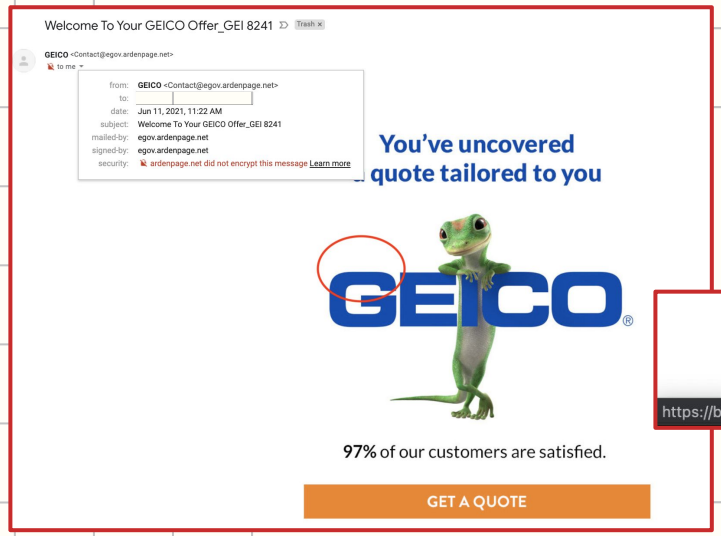
Hello friend. I'm honor to offer you collaboration with Maison Goyard Couture.
Goyard makes exclusive leather bags, accessories and other handmade goods.
New collection Spring / Summer 2021 soon gonna release & we happy if You pick any product you liked from our new desktop catalogue.
Would you like to be part of Maison Goyard history?

--
With best regards, Nita Novack,
Commercial manager of Maison Goyard.

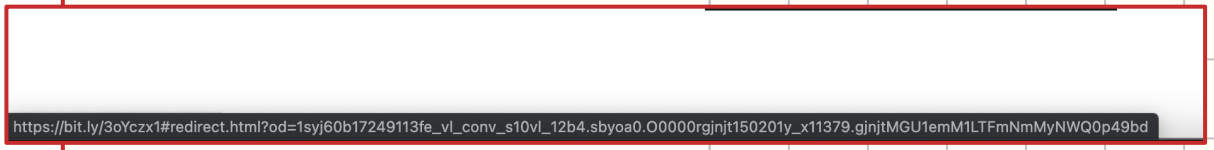
Reply Forward

1. **Who** is sending the email?
2. **What** is their goal?
3. **Where** is it coming from?

What to Look For, Again



Hover over the link! Does it want to take you to somewhere suspicious???



1. **Who** is sending the email?
2. **What** is their goal?
3. **Where** does it want to take me??

Fetish Mining

what is fetish mining?

The act of soliciting fetish content from somebody **without** them knowing the true purpose, and **without** their informed consent.

Is this Kink Shaming?

No. People are allowed to have kinks and unusual fetishes. However, if they are looking for content to satisfy their fetish, it is completely wrong to manipulate strangers into creating that content for them.

fetish mining signs to watch out for

- They are **persistent** and **fixated**, asking the same question over and over again.
- Their account tries to masquerade as an **un-threatening** person - usually as a **young girl**.
- They may try to pose it as a **"random"** or **"spontaneous"** topic.

They thrive on plausible deniability.

Trust your gut - If it feels weird, their intentions may be malicious

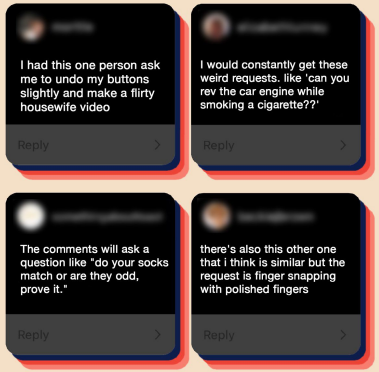
@beckitcruel

PEOPLE HAVE FETISHES. IT'S ALLOWED. WHAT'S THE PROBLEM?

FETISH MINING THRIVES AND DELIGHTS IN THE KNOWLEDGE THAT IT PREYS ON UNASSUMING STRANGERS.

The people who are targeted cannot give **informed consent** when participating in the fetish, because they are not informed that the request is **for** a fetish in the first place.

It's exploitative.



@beckitcruel

Popular Content Creator Scams

Popular Brands

- If it looks too good to be true, it probably is.
- Who is sending the email? Is it coming from a legitimate email address?
- Never download anything without scanning for potential viruses. If you don't have a software that does this, don't take the risk!

Congratulations! You've Won!

- "Congratulations, you've won the opportunity to join our affiliate program from Gucci. Click the link in the email NOW to apply."
    - Any indication of "haste" is usually a phish.
    - Hover over the link - is the URL taking you to Gucci.com or is it taking you to a Bit.ly link? If the latter, don't click it.

Popular Scams In General

Asking for PII (Personally Identifiable Information)

- Never share PII via email or online. This means your ID, passport, username/password, credit card number, banking/routing number. Any of this information coupled with your contact information is PII. Some of it is PII on its own.

Giftcards

- A friend of mine had an aunt who was told they would be approved for a $500,000 loan if they sent them $10,000 in gift cards. REAL BUSINESSES DO NOT DO BUSINESS VIA GIFT CARDS.

Ways to Protect Yourself

VPN

"A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks." (Kapersky)

Password Manager

"Attacks work because many people re-use the same password on multiple websites. Password managers makes it possible and easy to use a different random password for every account" (Stuart Schechter)

Use two-factor authentication or two-step verification

From your email to your social media sites, set it up.

Do's

Do

Implement a VPN.

Do

Be careful about how much information you share online.

Do

Keep your devices updated.

Don'ts

Don't

Text or email your credit card number, SSN or any other PII.

Don't

Use the same password everywhere.

Don't

Open up spam emails. Delete them right away!

Security Awareness, Online & Offline

If you receive a spam or phishing email, delete it

- I had a friend who would open up the fake Amazon email and go to the website and try to “unsubscribe” herself from the mailing list. Long story short: it didn’t work and she is also out $168.

Cover your webcam

- There is a reason why Mark Zuckerberg does it.

Always look for misspellings or issues with grammar/punctuation

- This is oftentimes an indication of malicious activity.

From: Admin <erikaquintanat@gmail.com>
Date: February 27, 2013, 4:22:24 PM CST
To: undisclosed-recipients:;
Subject: WARNING!

Dear User;

Due to the high influx of registration recorded on our mail database, would be doing some re-validation exercise on our database to know the number of active accounts that still exist so as to provide http://pp.pierregaragiste.com/ more active e-mail services.

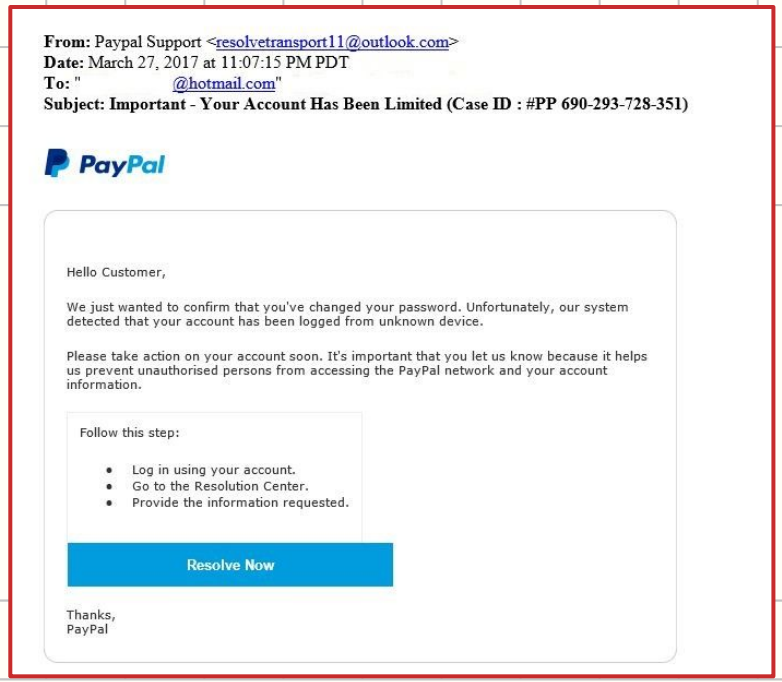
Click to follow link

Please visit our account validation webpage,Kindly CLICK HERE and carefully fill the required information listed in order to continue using your email account(s).

WARNING! Any account owner that refuses to update his/her account after five (5) days of receipt of the notification, will be disabled from our email database.

Thanks for your cooperation in advance!
Web-mail Team.

In the above example, you can see that although the email is from "Admin" the email is from a Gmail account. Also look at the issues with punctuation, and the sense of urgency in the email. The link also goes to an unknown domain.



From: Paypal Support <resolvetransport11@outlook.com>
Date: March 27, 2017 at 11:07:15 PM PDT
To: " @hotmail.com"
Subject: Important - Your Account Has Been Limited (Case ID : #PP 690-293-728-351)

PayPal

Hello Customer,

We just wanted to confirm that you've changed your password. Unfortunately, our system detected that your account has been logged from unknown device.

Please take action on your account soon. It's important that you let us know because it helps us prevent unauthorised persons from accessing the PayPal network and your account information.

Follow this step:

- Log in using your account.
- Go to the Resolution Center.
- Provide the information requested.

Resolve Now

Thanks,
PayPal

In the above example, you can see that although the email is from "PayPal Support" the email is from an Outlook account. Look at the sense of urgency in the email and the steps indicated are ones that would share PII.

Additional Resources

- Internet Safety Rules (Kapersky).
- 20 internet safety tips and checklist to help families stay safer online (Norton).
- How To Recognize and Avoid Phishing Scams (FTC).
- Phishing Attack Prevention: How to Identify & Avoid Phishing Scams (Digital Guardian).

- Nord VPN
  - https://nordvpn.com/lily (I have a link!)
  - Coupon code: lily (I also have a coupon code!)

- Best firewall of 2021: free, paid software and services (TechRadar).

Thanks!

Do you have any questions?

@lillianadee on IG/Twitter
Lily Whispers ASMR on
YouTube

Glossary

Social Engineering - (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Security Awareness - Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

Fetish Mining - the act of soliciting fetish content from somebody without them knowing the true purpose, and without their informed consent.

Phishing - Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

VPN - A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Firewall - a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Content Creator Reminders

1. You do not owe anyone anything.
2. You are entitled to your privacy.
3. What you wear, how you speak or where you make content, does not give people the right to harass or intimidate you.
4. There are attorneys and organizations that advocate for content creators such as Revision Legal and DoNotPay.
5. Online harassment is criminalized in many states and perpetrators can be convicted.
6. Self-taken photos—nude or not—are owned by the photographer, so a website displaying those photos without consent is violating copyright. You can seek upwards of $2,000,000 if you pursue people who leak content.