norton™

Phictionary

The phishing dictionary every digital citizen should read.

Table of Contents

Foreword

Michal Pechoucek
CTO at Gen™

Consumers are at the center of modern-day cybercrime. In 2023, scams and phishing attacks targeting consumers have been responsible for two-thirds of all cyber-attacks worldwide, according to Gen threat data. Pound-for-pound, there is more to gain by exploiting the flaws inherent in human beings than the flaws found in software and systems of companies.

This change in approach to cybercrime has coincided with a shift in the sophistication of phishing attacks. Older generations will remember the early days of scams which were often riddled with language and contextual errors that made them easy to spot. Today, cybercriminals are using Artificial Intelligence (AI) and tools such as ChatGPT to create highly targeted, error-free communications. As a result, the success rate of phishing is increasing.

To neutralize this, Cyber Safety's approach to protection needs to change too. It's no longer enough to protect weaknesses in devices with software, we need to protect the individual, something I call human-centered safety. Despite the bad intentions of cybercriminals to use AI to carry out attacks, it has a critical role to play in the detection of scams, and for over a decade Norton has been integrating AI into its products to help make the internet a safer place. But at the same time, we are focused on the human factor of online safety through education, which we believe will help to reduce the risk of human error.

As the name might suggest, Phictionary is a dictionary of phishing attacks recently detected and blocked by Norton, and we're exposing them to help you spot the tell-tale signs of suspicious communications designed to steal your personal information. As advocates for the empowerment of Digital Freedom for everyone, everywhere, Phictionary also includes a list of top tips that will help you decide what is, and what isn't, a phishing attack if you come across one.

Phictionary needed to exist to help correct a problem that's become normal. I really hope you find it useful.

Stay safe.

What is Phishing?

Phishing is a form of fraud that attempts to persuade people to voluntarily give up sensitive personal information by pretending to be a trustworthy source, such as a bank.

Phishing over email is the most common method, but other forms of electronic communications including text, video, websites and imagery can also be used to launch an attack.

Usually, the intent of a phishing attack is to obtain passwords to important accounts, capture credit card numbers or download malware to devices that could be used to eavesdrop or lock computers and files until a ransom is paid.

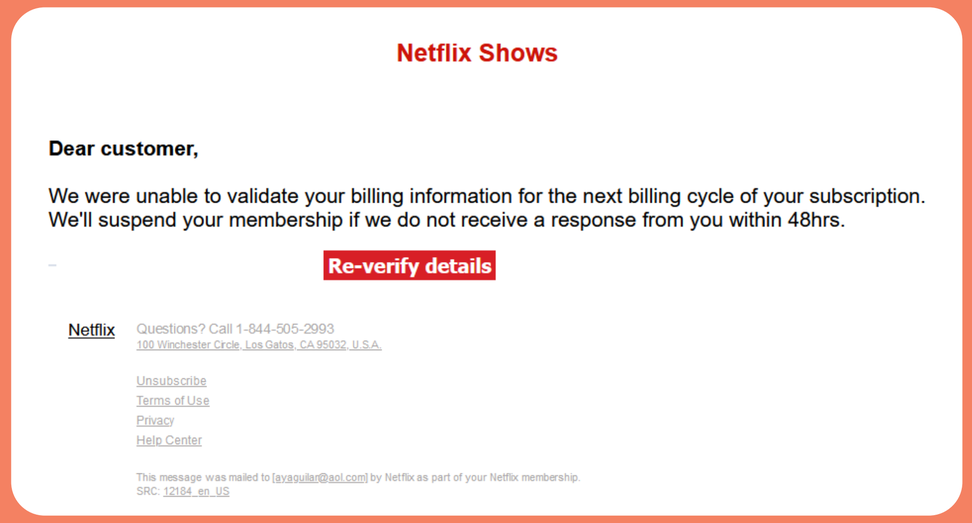
Phishing is still one of the most effective scams in the book, so we decided to expose some of the most common examples...

Account Information Alert

ə'kaʊnt ɪnfər'meɪʃən ə'lɜrts / noun

01. **An email or text sent to an individual by a service provider they are signed up with.**
Your Netflix membership has been ended, because we're having some trouble with your current account information.

02. **A scam that involves notifying a recipient of the need to update their account information, usually payment details.**



Account Suspension

ə'kaʊnt sə'spɛnʃən / verb

01. **A message received asking the recipient to restore their suspended account.**
Your Apple Pay has been suspended, please update your details by visiting: <|url|>

02. **A fake message addressed to an individual asking them to complete account recovery within a specific time period otherwise it will result in permanent suspension.**
We temporarily place your Paypal suspended, To restore follow instruction below. <|url|> Please complete the recovery within 2 days otherwise Paypal account permanently suspended. We are sorry for any inconvenience has caused. Thank you for your attention.

Account Verification

vɛrəfə'keɪʃən / noun

01. **A fraudulent email sent by scammers that looks like a message from a contact of a well-known entity with the goal to extract account login credentials.**
New login detected from: [Country name] Windows 10 Follow link below to unlock your account: <|url|> verify your account within 24 hours or your PayPal account will be terminated permanently. Regards, PayPal

Credit Crises

krɛdət kraɪsiz / noun

01. **A hoax financial reminder designed to steal personal and financial information.**
Reminder: If overdue records are not processed, it will affect your credit.

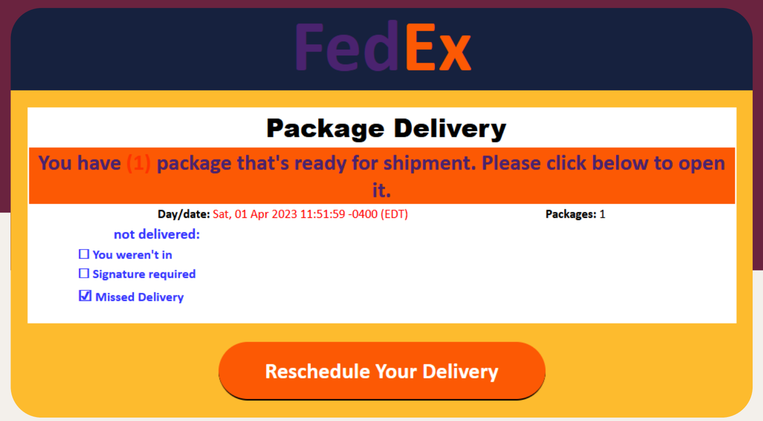
02. **A high priority text message or email threatening a credit rating downgrade.**
Important: Your credit will also be affected if past due records expire.

Delivery Mishap

dɪˈlɪvəri mɪsˌhæps / verb

01. **A fraudulent message faking an attempted delivery designed to extract personal information from the target.**
Our driver attempted to deliver your shipment today but no one was home. To reschedule a new delivery date, visit: <|url|>

02. **A text or email posing as a legitimate delivery company designed to trick someone into sharing information unknowingly.**
Your package cannot be delivered due to an incorrect house number.



Login Attempts

loginəˈtɛmpts / verb

01. **A message notifying the receiver that an unknown user has tried to access their account.**
CommBank Alert: A login was made from an Unknown Location: Melbourne, VIC. Not you? Please review now visit: <|url|>

02. **An attempt to trick somebody into thinking their account has been hacked, to convince them to share personal information.**
RBC Alert : Your online account is temporarily locked due to an unusual sign in attempt. Please login and confirm your information. <|url|>

Malware Threats

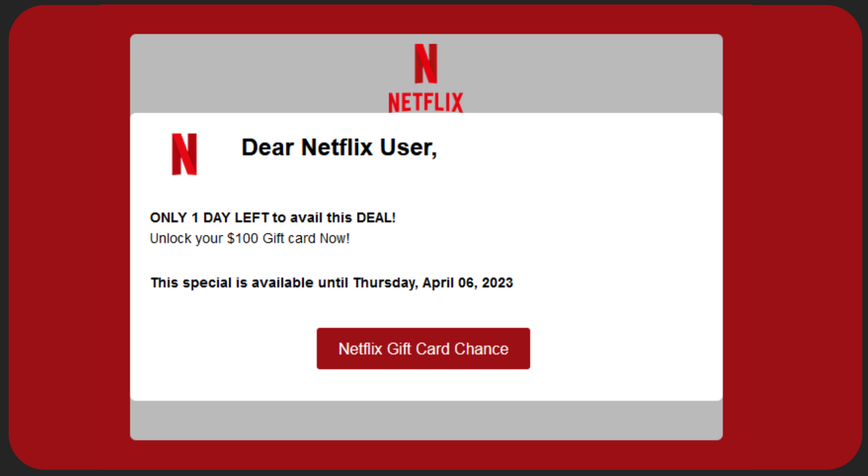
mæl¸wɛrθrɛts / noun

01. **A technique used by cybercriminals to trick people into thinking their device has been infected with malware.**
DANGER: A THREAT has INFECTED your LAPTOP! ACT NOW to PROTECT your CONFIDENTIAL FILES at <|url|>

Random Offer

rændəm ɔfərz / noun

01. **A scam designed to spread malware or obtain personal information by showing an attractive offer which includes a link to a malicious website to claim it.**
You Can Get PAID $100 for taking this 2-minute Survey!



Scare Tactic

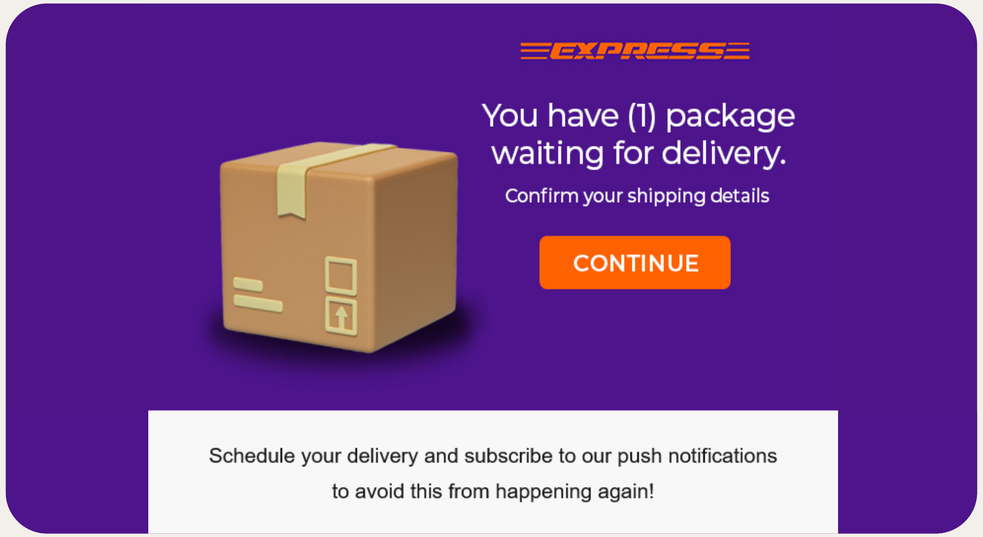
skɛr'tæktɪks / verb

01. **A common scam tactic that often uses fearmongering and urgency to steal personal or financial information.**
Your payment is overdue. Please avoid your fine charge please see <|url|>

Shipping Scams

ʃɪpɪŋ skæmz / noun

01. **A message received by a customer detailing delivery information and requesting delivery or payment preferences.**
Hi Your FEDEX parcel with tracking <|number|> is waiting for you to set delivery preferences: <|url|>

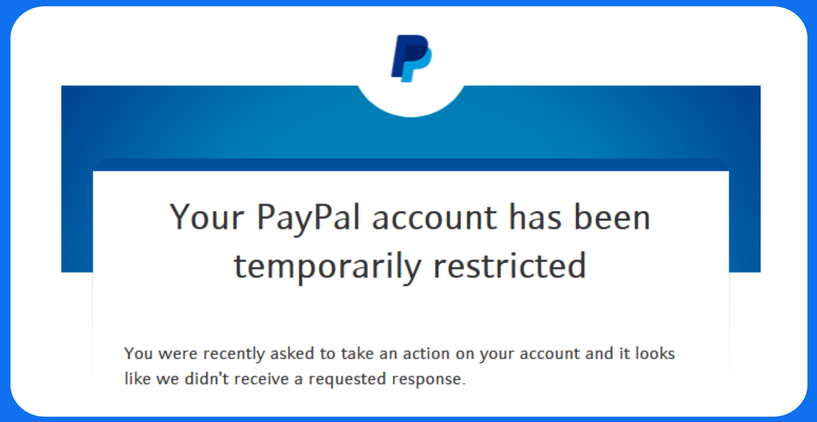


Suspicious Activity

səˈspɪʃəs ækˈtɪvəti / verb

01. **A phrase that refers to a type of email scam targeting online customers.**
Amazon: your account has been locked due to suspicious activity: <|url|>. Click the link below to unlock your account.

02. **A phrase referring to an email that appears to be sent directly from an online store, notifying the recipient that their personal account has been locked.**
Coinbase: your account has been locked due to suspicious activity. Click the link below to unlock your account: <|url|>



Tax Refund

tæksəz riˌfʌnd / noun

01. **A message from a copycat organization or individual attempting to steal money by offering fake refunds.**
[Inland Revenue] You have a pending refund. Please collect it now at: <|url|>

Tax Scam

tæks skæm / noun

01. **A spoof message masked as a revenue or customs company.**
myGov: Your income return of [amount] could not be processed due to insufficient information supplied please update immediately at <|url|>

Toll Scam

toʊl skæm/ noun

01. **A fraudulent attempt to gather banking details and steal money by alerting people to fake motorway fines.**
eFlow: You have been recorded using the motorway without paying the appropriate charge(s) of 6.40 visit <|url|> or an additional fine of 97.50 will be sent to your home address.

Our Recommendations to You

By now, you should be familiar with some of the most common types of phishing scams and the language they use. While some may appear obvious, phishing scams are becoming harder to identify with cybercriminals timing their attacks, personalizing their messages, and utilizing advanced technologies to increase their success rate. Here's what to look out for:

It sounds too good to be true
Beware of emails promising you free money or strange websites that are selling incredible products at unbelievable prices. If it looks too good to be true, it probably is.

A bank is asking for personal financial information
Banks won't ask for sensitive information by email or phone. Never supply this information in response to an email.

Poor spelling and grammatical errors
If an email is littered with spelling errors or strange phrasing, this should always be a red flag.

A generic greeting
If an email opens with generic greetings like "Dear Sir or Madam," it can be a sign that it's a phishing template that's been sent to multiple targets.

Emails from strangers
If you receive unsolicited emails from complete strangers or providers that you don't use, it's probably best to delete it. If you do open it, avoid clicking on any links or attachments.

It calls for immediate action
A common trick to get you to act is to create a false sense of urgency. It might threaten that an account will be deleted or claim that you've been hacked but it's just a way for scammers to get you to act without thinking.

Misspelled email addresses or domain names
If an email looks suspicious, always check the sender address or domain name for signs that it may be fake. It can be easy to miss these subtle details if you act on impulse.

It doesn't make sense
If you get an email claiming that you've just won a lottery that you never entered, then something is obviously up.

Keep this checklist close by and refer to it whenever you receive any communication that looks suspicious. If you're in doubt, erring on the side of caution and scrutinizing the message you've received will help you stay safe online and protect your personal information from cybercriminals. **For an extra layer of protection, install a reputable antivirus with anti-phishing technology, such as Norton 360.**

Get Protection

Disclaimer

All examples provided are real phishing samples found in the wild, not generated by Norton.
Any logos or trademarks displayed are the registered trademarks of the respective brands.

About Norton

Norton is a leader in Cyber Safety, and part of Gen™, a global company dedicated to powering Digital Freedom with a family of trusted consumer brands. Norton empowers millions of individuals and families with award-winning protection for their devices, online privacy, and identity.