THE INTERNET SURVIVAL GUIDE

for homeowners



What you'll find in this guide:

- Know Your Surroundings
- Your Survival Kit
- Your Biggest Threats
- Emergency Response

Powered by PHIN

KNOW YOUR SURROUNDINGS

Owning a home gives scammers plenty to work with—your address, property records, utility providers, deliveries, mortgage, contractors, and even the devices inside your house can all provide opportunities to make a scam seem convincing.

Owning a home is a luxury experienced by billions of people, and ~6 millennials. If you're lucky enough to be one of them, congratulations! You're a homeowner. Here's what you should know:

What do these mean?

Phishing: A fake email that tricks you into clicking, sharing info, or sending money.

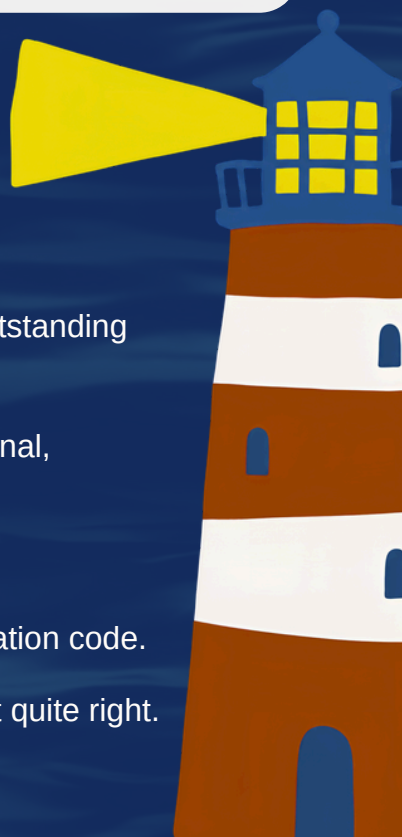
Smishing: Phishing by text message.

MFA (multi-factor authentication): An extra check at log-in, like a code sent to your phone.

Smart device: An internet-connected doorbell, camera, thermostat, TV, speaker, or appliance.

Malware: Harmful software that steals info, spies on you, or damages devices.

Major red flags to look out for:



🚩 **Urgency:** Pay immediately or your power will be disconnected, delivery returned, account closed, or opportunity lost.

🚩 **Unexpected payments:** Someone suddenly wants a deposit, fee, or outstanding bill paid.

🚩 **Changed payment details:** A contractor, attorney, real estate professional, or other company suddenly provides new banking instructions.

🚩 **Unusual payment methods:** Gift cards, crypto, or wire transfers.

🚩 **Passwords and codes:** Someone asks for login credentials or a verification code.

🚩 **Something looks off:** An email, website, phone number, or invoice isn't quite right.

YOUR SURVIVAL KIT

For help setting anything up, reach out to your IT provider or someone you trust.

Use different passwords. Your email, mortgage, utilities, security cameras, and online shopping accounts shouldn't *all* share the password you've used since 2014 with your mom's birthdate and the name of your family dog.

Use a password manager. A password manager securely creates and stores strong passwords for you. That makes using a different password for everything considerably easier.

Secure your Wi-Fi. Replace the default password with a strong one and only share it with people you trust.

Set up MFA wherever possible, especially for email, banking, and smart-home accounts. A stolen password shouldn't be enough to get someone inside. Digitally, we mean. Although the same principle applies to your front door.

Turn on account alerts so you're notified of unusual activity.

Update smart devices. Cameras, doorbells, TVs, thermostats, speakers, and other smart devices need updates too—which often includes security updates. Turn on automatic updates if they're available.

Know who you're hiring. Recommendations from people you trust are highly encouraged, but you should still always do your own research to ensure your contractor is reliable and will actually complete the job.

Know who you're paying. Keep trusted contacts for contractors, utilities, and your mortgage. If someone suddenly changes their payment details, verify the change using contact information you already have.



Before you click, pay, give someone account access, or hand off information:

ALWAYS PAUSE & PONDER

Who is this?

Do you actually know who's contacting you? A company name, logo, caller ID, or familiar email display name isn't proof by itself.

What do they want?

Money? Banking information? A password? A verification code? Access to your computer or home? The more valuable the request, the more carefully you should check it.

Why are they reaching out & does it make sense?

- Were you expecting this bill, delivery, contractor, or message?
- Does the amount make sense?
- Have you ever dealt with this company before?

When do you need to respond?

Your electricity is about to be disconnected. The contractor needs a deposit today. Your package will be returned in two hours. Conveniently, scammers often have a reason you can't stop and think. **Urgency is a reason to slow down, not speed up.**

Where can I verify it?

Contact the company or person using a phone number, app, website, or contact details you already trust. Don't use the suspicious message to verify the suspicious message.

YOUR BIGGEST THREATS

1 "WE CAN FIX YOUR ROOF TODAY"

After a storm, a contractor offers urgent repairs but wants a big deposit before you can check their business, references, or insurance. They may disappear with the money or leave you with poor or unfinished work.

What should you do? Don't let urgency decide. Research contractors, get written estimates, check references, and avoid large upfront payments.

2 "OUR PAYMENT DETAILS HAVE CHANGED"

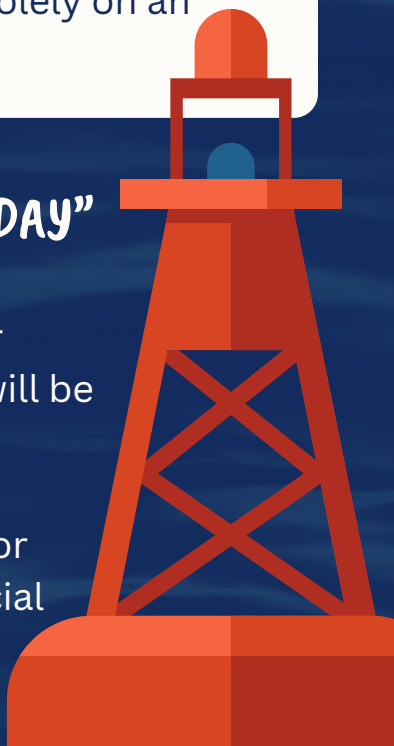
You're expecting to pay a contractor, cover closing costs, or pay another large house-related bill when an email arrives with new payment instructions. It looks genuine because criminals may have copied or compromised a real email account.

What should you do? Verify payment details directly with someone you already know using trusted contact information. Never rely solely on an email telling you where to send a large payment.

3 "YOUR POWER WILL BE DISCONNECTED TODAY"

Someone claiming to represent your electricity, gas, water, or another utility says you're behind on payments and service will be disconnected unless you pay immediately.

What should you do? Don't pay through an unexpected call or message. Contact your utility provider yourself using its official app, website, bill, or a trusted phone number.





"WE COULDN'T DELIVER YOUR PACKAGE"

A text or email claims there's a problem with a delivery and asks you to click a link to rearrange it or pay a small fee. The website may look convincing but is designed to steal payment or personal information.

What should you do? Check deliveries through the retailer's or carrier's official app or website rather than using the link in the message.



"YOUR SMART HOME ISN'T THAT PRIVATE"

Cameras, doorbells, speakers, thermostats, and TVs connect to your home network and online accounts. Weak or reused passwords, outdated software, and poorly secured accounts make them easier to compromise.

What should you do? Use unique passwords and MFA where available, install updates, and change default passwords when setting up new devices.



"WE KNOW YOU JUST MOVED"

Moving makes you an attractive target. You're expecting messages from banks, utilities, delivery companies, contractors, and insurers, which makes fake ones harder to spot.

What should you do? Be extra cautious with unexpected moving-related messages. Contact companies independently and avoid announcing your new address publicly.

WHEN IN DOUBT, CONTACT THE COMPANY YOURSELF.

OH, CRAP. I FELL FOR A SCAM.

Now what?

Whether you paid a fake contractor, entered card details on a fake delivery site, or handed over a password, acting quickly can help limit the damage.

STEP 1

Stop communicating with the scammer and don't send more money or info, even if they claim it will fix the problem or recover what you've already lost.

STEP 2



If you sent money or shared payment info, contact your bank, card provider, or payment service immediately.



If you shared a password, change it anywhere you've reused it and enable MFA. Start with your email.



If a smart-home account or device was compromised, change the account and device passwords, install available updates, and remove any users or devices you don't recognize.

STEP 3

Keep emails, messages, invoices, phone numbers, receipts, payment information, screenshots, and any other records. If a contractor or other person has physically visited your property, make a note of names, company details, vehicle information, and anything else you remember.

STEP 4

Report fraudulent accounts or messages to the appropriate authorities. If money is involved, make sure your financial provider knows what happened.

In the US, report fraud at ReportFraud.ftc.gov and internet crime at ic3.gov.